

MEMORY CARD

Publication number: WO02099742

Publication date: 2002-12-12

Inventor: MIZUSHIMA NAGAMASA (JP); TSUNEHIRO TAKASHI (JP); TSUNODA MOTOYASU (JP); TANAKA TOSHIO (JP); KATAYAMA KUNIHIRO (JP); KIMURA KOUICHI (JP); HATANO TOMIHISA (JP)

Applicant: HITACHI LTD (JP); MIZUSHIMA NAGAMASA (JP); TSUNEHIRO TAKASHI (JP); TSUNODA MOTOYASU (JP); TANAKA TOSHIO (JP); KATAYAMA KUNIHIRO (JP); KIMURA KOUICHI (JP); HATANO TOMIHISA (JP)

Classification:

- international: **G06F21/00; G06F21/00;** (IPC1-7): G06K19/073; G06F12/14

- european: G06F21/00N9F

Application number: WO2002JP05236 20020529

Priority number(s): JP20010167617 20010604

Also published as:



EP1396815 (A1)

US2004177215 (A1)

CN1505802 (A)

Cited documents:



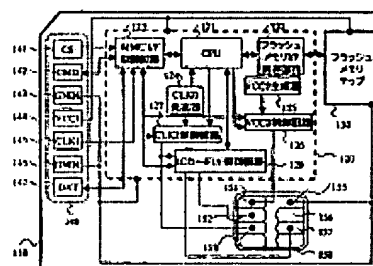
JP5314013

JP8055200

Report a data error here

Abstract of WO02099742

Security of a storage apparatus is increased. A memory card includes a flash memory chip, an IC card chip capable of executing security processing (encryption, decryption, etc.), and a control chip for controlling data read/write from/to the flash memory chip and the IC card chip in response to a request of the host.



111...HOST I/F CONTROL CIRCUIT
123...FLASH MEMORY I/F CONTROL CIRCUIT
131...FLASH MEMORY CHIP
134...CLOCK OSCILLATOR
135...A/D CONVERTER
136...A/D CONTROL CIRCUIT
137...CLOCK CONTROL CIRCUIT
138...IC CARD I/F CONTROL CIRCUIT

Data supplied from the **esp@cenet** database - Worldwide

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2002 年 12 月 12 日 (12.12.2002)

PCT

(10) 国際公開番号
WO 02/099742 A1

- (51) 国際特許分類⁷: G06K 19/073, G06F 12/14
- (21) 国際出願番号: PCT/JP02/05236
- (22) 国際出願日: 2002 年 5 月 29 日 (29.05.2002)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願2001-167617 2001 年 6 月 4 日 (04.06.2001) JP
- (71) 出願人 (米国を除く全ての指定国について): 株式会社日立製作所 (HITACHI, LTD.) [JP/JP]; 〒101-8010 東京都千代田区神田駿河台四丁目6番地 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 水島 永雅 (MIZUSHIMA, Nagamasa) [JP/JP]; 〒215-0013 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内 Kanagawa (JP). 常広 隆司 (TSUNEHIRO, Takashi) [JP/JP]; 〒215-0013 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内 Kanagawa (JP). 角田 元泰 (TSUNODA, Motoyasu) [JP/JP]; 〒215-0013 神奈川県

川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内 Kanagawa (JP). 田中 紀夫 (TANAKA, Toshio) [JP/JP]; 〒212-0058 神奈川県川崎市幸区鹿島田890番地 株式会社日立製作所金融システム事業部内 Kanagawa (JP). 片山 国弘 (KATAYAMA, Kunihiro) [JP/JP]; 〒187-0022 東京都小平市上水本町五丁目20番1号 株式会社日立製作所半導体グループ内 Tokyo (JP). 木村 光一 (KIMURA, Kouichi) [JP/JP]; 〒215-0013 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内 Kanagawa (JP). 幡野 富久 (HATANO, Tomihisa) [JP/JP]; 〒215-0013 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内 Kanagawa (JP).

(74) 代理人: 浅村 皓, 外 (ASAMURA, Kiyoshi et al.); 〒100-0004 東京都千代田区大手町2丁目2番1号 新大手町ビル331 Tokyo (JP).

(81) 指定国 (国内): CN, JP, KR, US.

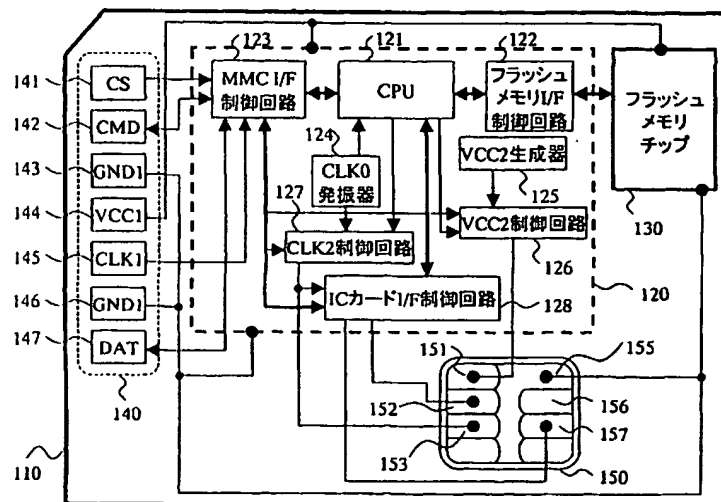
(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

添付公開書類:
— 国際調査報告書

[続葉有]

(54) Title: MEMORY CARD

(54) 発明の名称: 記憶装置



123...MMC I/F CONTROL CIRCUIT
122...FLASH MEMORY I/F CONTROL CIRCUIT
130...FLASH MEMORY CHIP
124...CLK0 OSCILLATOR
125...VCC2 GENERATOR
126...VCC2 CONTROL CIRCUIT
127...CLK2 CONTROL CIRCUIT
128...IC CARD I/F CONTROL CIRCUIT

(57) Abstract: Security of a storage apparatus is increased. A memory card includes a flash memory chip, an IC card chip capable of executing security processing (encryption, decryption, etc.), and a control chip for controlling data read/write from/to the flash memory chip and the IC card chip in response to a request of the host.

[続葉有]

WO 02/099742 A1



2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

本発明は、記憶装置のセキュリティを向上することを目的とする。そして、本発明は、フラッシュメモリチップと、セキュリティ処理（暗号化や復号化等）を実行可能なICカードチップと、ホストからの要求に応じて、フラッシュメモリチップ及びICカードチップへのデータの読み書きを制御するコントローラチップとを備える。

明 細 書

記憶装置

5 技術分野

本発明は、セキュリティ機能を搭載した記憶装置及びその記憶装置が挿入可能なホスト機器及びその記憶装置が挿入されたホスト機器に係り、特に、電氣的に消去可能な不揮発性メモリ（例えば、フラッシュメモリ）を有するメモリカード及びそのメモリカードが挿入可能なホスト機器及びそのメモリカードが挿入されたホスト機器に関する。

背景技術

- ＩＣカードは、プラスチックカード基板中にＩＣ（集積回路）チップを埋め込んだものであり、その表面にＩＣチップの外部端子を持つ。ＩＣチップの外部端子には電源端子、クロック端子、データ入出力端子などがある。ＩＣチップは、
- 15 接続装置が外部端子から電源や駆動クロックを直接供給することによって動作する。ＩＣカードは外部端子を通して端末機などの接続装置との間で電気信号を送受信することにより、接続装置と情報交換をおこなう。情報交換の結果として、
- ＩＣカードは計算結果や記憶情報の送出、記憶情報の変更をおこなう。ＩＣカードは、これらの動作仕様に基づいて、機密データ保護や個人認証などのセキュリ
- 20 ティ処理を実行する機能を持つことができる。ＩＣカードは、クレジット決済やバンキングなど機密情報のセキュリティが必要とされるシステムにおいて、個人識別のためのユーザデバイスとして利用されている。

- セキュリティシステムにおいて利用されるＩＣカードは、秘密情報を用いて演算を行う際に、その秘密情報あるいはその秘密情報を推定できるような情報を外
- 25 にももらさないように設計される必要がある。すなわち、耐タンパ性を持つことが必要とされる。このような外にももらしてはならない秘密情報を解析する攻撃方法としては、タイミング解析、電力差分析、故障利用解析などが知られている。

タイミング解析は、暗号処理時間が秘密情報の内容に依存して異なる場合、その時間差を統計的に解析して秘密情報を推定する攻撃法である。暗号アルゴリズム

- ムを実装する際、処理時間の短縮やプログラムサイズの縮小を目的として、秘密情報の内容に依存して不要処理をスキップしたり分岐処理を行ったりするような最適化を適用することがある。このような最適化を適用すると、暗号処理時間が秘密情報の内容に依存して異なる。そのため処理時間を見ることで秘密情報の内容
- 5 容を推定できる可能性がある。

電力差分析は、暗号処理の実行中にＩＣカードの電源端子から供給される電力を測定し、そこから消費電力の差分を解析することにより秘密情報を推定する攻撃法である。

- 故障利用解析は、ＩＣカードの計算誤りを利用した攻撃法である。ＩＣカード
- 10 に一過性の故障あるいは他の機能に影響を与えない範囲の限定的な障害を与え、ＩＣカードに攻撃者の望む異常な処理を行わせる。ＩＣカードに高電圧を加えたり、瞬間的にクロック周波数や駆動電圧を変動させることにより故意にエラーを発生させた場合、その結果得られる誤った計算結果と正しい計算結果から秘密情報が得られる可能性がある。
- 15 ＩＣカードは、実用上、これらの攻撃法に対する対策手段を持たなければならない。

発明の開示

本発明の第１の目的は、セキュリティを向上した記憶装置を提供することである。

- 20 本発明の第２の目的は、製造が簡略化された記憶装置を提供することである。

第１の目的を達成するために、本発明は、データを記憶可能なメモリと、データを記憶可能でかつデータのセキュリティ処理を実行可能な処理装置と、外部のホスト機器からのコマンドに基づいて、メモリと処理装置とを制御するコントローラとを備える。

- 25 第１の目的を達成するために、本発明は、フラッシュメモリチップと、コントローラと、外部端子と、ＩＣチップとを備え、ＩＣチップのグランド端子は外部端子に接続され、ＩＣチップの電源入力端子とリセット入力端子とクロック入力端子とデータ入出力端子は、コントローラに接続される。

第２の目的を達成するために、データを記憶可能なフラッシュメモリチップと、

フラッシュメモリチップへのデータの読み書きを制御するコントローラと、ＩＣチップとを備え、ＩＣチップは、認証機関によって予め認証された後に搭載される。

本発明の他の目的、特徴及び利点は添付図面に関する以下の本発明の実施例の記載から明らかになるであろう。

図面の簡単な説明

第１図は、本発明を適用したMMCの内部構成を示す図である。

第２図は、本発明を適用したMMCのホスト機器の内部構成、およびホスト機器とMMCとの接続状態を示す図である。

10 第３図は、ＩＣカードチップのコールドリセット時の信号波形を示す図である。

第４図は、ＩＣカードチップのウォームリセット時の信号波形を示す図である。

第５図は、ＩＣカードチップのＩＣカードコマンド処理時の信号波形を示す図である。

第６図は、ＩＣカードチップの非活性化時の信号波形を示す図である。

15 第７図は、ホスト機器によるMMCへのアクセスを示したフローチャートである。

第８図は、ＩＣカード制御パラメータとそれに対応するＩＣカードへの処理内容を示す図表である。

20 第９図は、ＩＣカードチップに対する第１次ＩＣカード初期化の詳細なフローチャートである。

第１０図は、ＩＣカードチップに対する第２次ＩＣカード初期化の詳細なフローチャートである。

第１１図は、非活性状態のＩＣカードチップに対するＩＣカード初期化時の信号波形を示す図である。

25 第１２図は、活性状態のＩＣカードチップに対するＩＣカード初期化時の信号波形を示す図である。

第１３図は、ＩＣカードチップによるセキュリティ処理の詳細なフローチャートである。

第１４図は、セキュリティ処理要求ライトコマンドを処理するときの信号波形

とフラッシュメモリチップアクセスを示す図である。

第15図は、ICカードチップによるセキュリティ処理実行時の信号波形とフラッシュメモリチップアクセスの一例を示す図である。

第16図は、セキュリティ処理結果リードコマンドを処理するときの信号波形
5 とフラッシュメモリチップアクセスを示す図である。

第17図は、インタフェース直通モードにおけるMMC外部端子とICカードチップ外部端子の対応関係を示す図である。

第18図は、インタフェース直通モードへ移行する処理とインタフェース直通モードから復帰する処理のフローチャートである。

10 第19図は、インタフェース直通モードへ移行する処理時の信号波形を示す図である。

第20図は、インタフェース直通モードから復帰する処理時の信号波形を示す図である。

第21図は、フラッシュメモリチップの内部構成を示す図である。

15 第22図は、本発明を適用したMMCの内部構成を簡単に示す図である。

第23図は、本発明を適用したMMCをコンテンツ配信に応用した例を示す図である。

第24図は、本発明を適用したSDカードの内部構成を簡単に示す図である。

20 第25図は、本発明を適用したメモリースティックの内部構成を簡単に示す図である。

第26図は、本発明のICカードチップの内部構成を示す図である。

第27図は、セキュリティ処理要求とセキュリティ処理結果の各データフォーマットの一例を示す図である。

発明を実施するための最良の形態

25 以下、本発明の一実施形態について説明する。

図22は、本発明を適用したMulti Media Card (Multi Media CardはInfineon Technologies AGの登録商標である。以下、「MMC」と略記する。)の内部構成図を簡単に表したものである。MMC1.1.0は、Multi

Media Card仕様に準拠するのが好ましい。MMC 110は、外部に接続したホスト機器220がMulti Media Card仕様に準拠したメモリカードコマンドを発行することによって、機密データ保護や個人認証などに必要な暗号演算をおこなうセキュリティ処理機能を持つ。ホスト機器220は、
5 例えば、携帯電話、携帯情報端末（PDA）、パーソナルコンピュータ、音楽再生（及び録音）装置、カメラ、ビデオカメラ、自動預金預払器、街角端末、決済端末等が該当する。MMC 110は、MMC外部端子140、コントローラチップ120、フラッシュメモリチップ130、ICカードチップ150を持つ。フラッシュメモリチップ130は、不揮発性の半導体メモリを記憶媒体とするメモリチップであり、フラッシュメモリコマンドによりデータの読み書きができる。
10 MMC外部端子140は7つの端子から構成され、外部のホスト機器220と情報交換するために、電源供給端子、クロック入力端子、コマンド入出力端子、データ入出力端子、グランド端子を含む。コントローラチップ120は、MMC 110内部の他の構成要素（MMC外部端子140、フラッシュメモリチップ130、ICカードチップ150）と接続されており、これらを制御するマイコンチップである。ICカードチップ150は、ICカードのプラスチック基板中に埋め込むためのマイコンチップであり、その外部端子、電気信号プロトコル、コマンドはISO/IEC 7816規格に準拠している。ICカードチップ150の外部端子には、電源供給端子、クロック入力端子、リセット入力端子、I/O入
15 出力端子、グランド端子がある。コントローラチップ120は、ICカードチップ150の外部端子からICカードチップ150にICカードコマンドを発行することによって、外部のホスト機器220から要求されたセキュリティ処理に必要な演算をおこなう。

図26は、本発明のICカードチップの内部構成を示す図である。ICカード
25 チップ150は、演算処理を行うためのCPU（マイコン）158と、データ（プログラムを含む。）を記憶するためのROM（Read Only Memory）159とRAM（Random Access Memory）160とEEPROM（Electrically Erasable Programmable ROM）162と、暗号／復号に関する処理を行うための暗号コプロセッサ163と、外部とデータを送受信するためのシリアルインター

フェース 161 とを備え、それらは、バス 164 によって接続される。そして、その暗号コプロセッサ 163 によって、ホスト機器 220 からのコマンドに応じて、IC カードチップ 150 自らが、セキュリティ処理を実行することが可能である。尚、暗号コプロセッサ 163（ハードウェア）の替わりに、プログラム 5（ソフトウェア）に従って CPU 158 がセキュリティ処理を実行してもよい。

一方、フラッシュメモリチップ 130 には、記憶素子を備えるが、マイコンは存在しない。セキュリティ処理は、例えば、IC カードチップ 150 内の記憶領域にデータが書き込まれるとき、又は、IC カードチップ 150 内の記憶領域からデータが読み出されるときに実行される。IC カードチップ 150 の EEPROM の記憶容量は、フラッシュメモリチップ 130 の記憶容量より小さい。但し、IC カードチップ 150 の EEPROM の記憶容量は、フラッシュメモリチップ 130 の記憶容量と同じでもよいし、大きくてもよい。

IC カードチップ 150 には、セキュリティ評価基準の国際標準である ISO / IEC 15408 の評価・認証機関によって認証済みである製品を利用する。一般に、セキュリティ処理をおこなう機能を持つ IC カードを実際の電子決済サービスなどで利用する場合、その IC カードは ISO / IEC 15408 の評価・認証機関による評価と認定を受ける必要がある。MMC にセキュリティ処理をおこなう機能を追加することによって MMC 110 を実現し、それを実際の電子決済サービスなどで利用する場合、MMC 110 も同様に ISO / IEC 15408 の評価・認証機関による評価と認定を受ける必要がある。本発明によれば、MMC 110 は、評価・認証機関によって認証済みの IC カードチップ 150 を内蔵し、その IC カードチップ 150 を利用してセキュリティ処理をおこなう構造を持つことにより、セキュリティ処理機能を得る。したがって、MMC 110 は ISO / IEC 15408 に基づくセキュリティ評価基準を容易に満足することができ、MMC にセキュリティ処理機能を追加するための開発期間を短縮することができる。

MMC 110 は、Multi Media Card 仕様に準拠した外部インタフェースを持つのが好ましい。MMC 110 は、一種類の外部インタフェースを通じて、標準メモリカードコマンド（フラッシュメモリチップ 130 へアクセ

スするためのコマンド)に加えて、セキュリティ処理を実行するコマンドを受け付ける必要がある。コントローラチップ120は、MMC110が受信したコマンドが標準メモリカードコマンドであるか、セキュリティ処理を実行するコマンドであるかによって、アクセスすべきチップを選択し、コマンド処理を分配する機能を持つ。本発明によれば、標準メモリカードコマンドを受信したならば、フラッシュメモリチップ130を選択し、これにフラッシュメモリコマンドを発行してホストデータを読み書きできる。また、セキュリティ処理を実行するコマンドを受信したならば、ICカードチップ150を選択し、これにICカードコマンドを発行してセキュリティ処理を実行することができる。

- 10 ICカードチップ150の外部端子は、グランド端子を除いて、電源供給端子、クロック入力端子、リセット入力端子、I/O入出力端子がコントローラチップ120に接続されている。

コントローラチップ120は、電源供給端子、クロック入力端子を通して、ICカードチップ150への電源供給、クロック供給を制御する。本発明によれば、
15 ホスト機器220からセキュリティ処理を要求されないときには、ICカードチップ150への電源供給やクロック供給を停止させることができ、MMC110の電力消費を削減することができる。

電源供給されていないICカードチップ150を、ICカードコマンドを受信できる状態にするには、まず、ICカードチップ150に電源供給を開始し、リ
20 セット処理(クロック供給の開始を含む)を施すことが必要である。例えば、コントローラチップ120は、MMC110がホスト機器220からセキュリティ処理を実行するコマンドを受信したのを契機に、電源供給端子を通してICカードチップ150への電源供給を開始してもよい。あるいは、コントローラチップ120は、セキュリティ処理を実行しないときもICカードチップ150への電
25 源供給を維持しておき、MMC110がホスト機器220からセキュリティ処理を実行するコマンドを受信したのを契機に、リセット入力端子を通してICカードチップ150のリセット処理をおこなってもよい。本発明によれば、コントローラチップ120は、セキュリティ処理を実行するコマンドを受信するまでICカードチップ150への電源とクロック両方の供給、あるいはクロック供給のみ

- を停止させておくことができる。したがって、MMC 110の電力消費を削減することができる。ICカードチップ150がスリープモードの動作をサポートしている場合は、セキュリティ処理を実行していない時にクロック供給のみを停止するだけでも電力消費を大幅に削減できる。これはISO/IEC 7816-3
- 5 規格により、電源電圧3VでのICカードの電気特性は、通常動作状態で最大50mA、クロック停止状態で最大0.5mAと規定されているためである。なお、スリープモードとは、クロック供給を止めても電源さえ供給していれば、ICカードチップ150の内部状態（コアCPUのレジスタやRAMに保持されたデータ）が保存される動作モードである。
- 10 コントローラチップ120は、ICカードチップ150のクロック入力端子を通してICカードチップ150に供給するクロック信号をMMC 110内部で発生し、その周波数、供給開始タイミング、供給停止タイミングを制御する機能を持つ。本発明によれば、MMC外部端子140のクロック入力端子のクロック信号と無関係にすることができるため、ホスト機器220によるタイミング解析、
- 15 電力差分解析、故障利用解析と呼ばれる攻撃法に対してセキュリティが向上する。
- 図21は、フラッシュメモリチップ130の詳細な内部構成を表している。フラッシュメモリチップ130は、ホストデータ領域2115と管理領域2110とを含む。ホストデータ領域2115は、セクタ単位に論理アドレスがマッピングされている領域であり、ホスト機器220が論理アドレスを指定してデータを
- 20 読み書きできる領域である。ホストデータ領域2115は、ユーザファイル領域2130とセキュリティ処理アプリケーション領域2120とを含む。ユーザファイル領域2130は、ユーザが自由にファイルデータを読み書きできる領域である。セキュリティ処理アプリケーション領域2120は、ホスト機器220がセキュリティ処理アプリケーションに必要なデータを格納する領域であり、ユー
- 25 ザが不正にアクセスしないように、ホスト機器220のセキュリティ処理アプリケーションが論理的にユーザアクセス制限をかける。ここに格納するデータとしては、ホスト機器220のアプリケーションプログラム、そのアプリケーション専用のデータ、セキュリティ処理に使用される証明書など（例えば、電子決済アプリケーションプログラム、電子決済ログ情報、電子決済サービス証明書など）

が可能である。本発明によれば、MMC 110が、ホスト機器220がセキュリティ処理をおこなう上で使用するデータをホスト機器220の代わりに格納するため、ホスト機器220にとって利便性が向上する。一方、管理領域2110は、コントローラチップ120がICカードチップ150を管理するための情報を格納する領域である。管理領域2110は、ICカード制御パラメータ領域2111、ICカード環境設定情報領域2112、CLK2設定情報領域2113、セキュリティ処理バッファ領域2114、セキュリティ処理ステータス領域2116とを含む。2111～2116の領域の詳細な使用法については後述する。

コントローラチップ120は、フラッシュメモリチップ130の管理領域2110のセキュリティ処理バッファ領域2114を、ICカードチップ150でセキュリティ処理を実行する際のメインメモリまたはバッファメモリとして利用する。ホスト機器220がセキュリティ処理を実行するコマンドによりMMC 110にアクセスした際に、MMC 110がホスト機器220からICカードチップ150に一度に送信できないほどの大きなサイズのセキュリティ関連データを受信したならば、コントローラチップ120はフラッシュメモリチップ130へのアクセスを選択し、そのデータを十分な容量を持つセキュリティ処理バッファ領域2114に一時的に格納する。ICカードチップ150に一度に送信できないほどのサイズは、ICカードコマンドの許容データサイズ（例えば、255バイト又は256バイト）を超えるサイズである。そして、コントローラチップ120はそれをICカードチップ150に送信できるサイズのデータに分割し、分割データをフラッシュメモリチップ130から読み出し、段階的にICカードチップ150に送信する。つまり、分割されたデータの読み出し、書き込みを繰り返す。本発明によれば、ホスト機器220にとって、大きなサイズのセキュリティ関連データを扱うことができるので、セキュリティ処理の利便性が向上する。

上記のセキュリティ処理バッファ領域2114を含む管理領域2110は、ホスト機器220が不正にアクセスしてセキュリティ処理を解析することができないように、コントローラチップ120により物理的にホストアクセス制限がかけられている。つまり、管理領域2110はホスト機器220が直接データを読み書きできない。本発明によれば、ホスト機器220がセキュリティ処理バッファ

領域 2 1 1 4 の内容を自由に読み出したり改ざんすることができないため、セキュリティ処理の信頼性や安全性が向上する。

図 2 3 は、MMC 1 1 0 を利用したセキュリティ処理の一例として、コンテンツ配信のセキュリティ処理を表したものである。コンテンツプロバイダ 2 3 1 0 は、MMC 1 1 0 を所有するユーザにコンテンツ 2 3 1 4 を販売する業者である。ホスト機器 2 2 0 は、この例では、コンテンツプロバイダ 2 3 1 0 とネットワークなどを介して接続することができる端末機である。ユーザは MMC 1 1 0 をホスト機器 2 2 0 に接続してコンテンツ 2 3 1 4 を購入する。以下、その手順を説明する。

- 10 まず、ホスト機器 2 2 0 は MMC 1 1 0 に、フラッシュメモリチップ 1 3 0 に格納されたユーザ証明書 2 3 2 1 を読み出すコマンドを発行する。MMC 1 1 0 のコントローラチップ 1 2 0 は、フラッシュメモリチップ 1 3 0 のセキュリティ処理アプリケーション領域 2 1 2 0 に格納されたユーザ証明書 2 3 2 1 を読み出し、それをホスト機器 2 2 0 に送信する。そして、ホスト機器 2 2 0 はそれをコンテンツプロバイダ 2 3 1 0 に送信する。コンテンツプロバイダ 2 3 1 0 はユーザ証明書 2 3 2 1 につけられたデジタル署名を検証する (2 3 1 1)。検証が成功したならば、乱数発生器によりセッション鍵を生成し (2 3 1 2)、それをユーザ証明書 2 3 2 1 から抽出したユーザ公開鍵によって暗号化する (2 3 1 3)。さらに、コンテンツ 2 3 1 4 をそのセッション鍵によって暗号化する (2 3 1 5)。
- 20 コンテンツプロバイダ 2 3 1 0 はステップ 2 3 1 3 の結果をホスト機器 2 2 0 に送信する。ホスト機器 2 2 0 は、ステップ 2 3 1 3 の結果をユーザ秘密鍵 2 3 2 2 によって復号するセキュリティ処理を要求するコマンドを、MMC 1 1 0 に発行する。コントローラチップ 1 2 0 は、ステップ 2 3 1 3 の結果をユーザ秘密鍵 2 3 2 2 によって復号する IC カードコマンドを、IC カードチップ 1 5 0 に発行する。IC カードチップ 1 5 0 は、ユーザ秘密鍵 2 3 2 2 によってステップ 2 3 1 3 の結果を復号して、セッション鍵を取得する (2 3 2 3)。ホスト機器 2 2 0 は、この復号処理が成功したかを示す情報を出力させるコマンドを MMC 1 1 0 に発行する。コントローラチップ 1 2 0 は、IC カードチップ 1 5 0 の出力する復号結果 (復号処理が成功したかを示す IC カードレスポンス) をも

とにしてホスト機器 220 の求める情報を構築する。そして、MMC 110 はその情報をホスト機器 220 に送信する。次に、コンテンツプロバイダ 2310 は、ステップ 2315 の結果を、ホスト機器 220 に送信する。ホスト機器 220 は、ステップ 2313 の結果をセッション鍵（ステップ 2323 によって取得した
5 鍵）によって復号するセキュリティ処理を要求するコマンドを、MMC 110 に発行する。コントローラチップ 120 は、ステップ 2315 の結果をセッション鍵によって復号する IC カードコマンドを、IC カードチップ 150 に発行する。IC カードチップ 150 は、セッション鍵によってステップ 2315 の結果を復号して、コンテンツ 2314 を復元する（2324）。コントローラチップ 12
10 0 は、このコンテンツ 2314 を IC カードチップ 150 から受信し、フラッシュメモリチップ 130 に書きこむ。ホスト機器 220 は、この復号処理が成功したかを示す情報を出力させるコマンドを MMC 110 に発行する。コントローラチップ 120 は、IC カードチップ 150 の出力する復号結果（復号処理が成功したかを示す IC カードレスポンス）をもとにしてホスト機器 220 の求める情
15 報を構築する。そして、MMC 110 はその情報をホスト機器 220 に送信する。ホスト機器 220 が、コンテンツを無事に受信したことをコンテンツプロバイダ 2310 に伝え、コンテンツプロバイダ 2310 はユーザ証明書に記載されたユーザにコンテンツ料金を課金する。ユーザは、ホスト機器 220 で MMC 110 内のフラッシュメモリチップ 130 に格納されたコンテンツ 2314 を読み
20 出して利用することができる。また、フラッシュメモリチップ 130 の記憶媒体に大容量のフラッシュメモリを使用すれば、多くのコンテンツを購入できる。

本発明によれば、コンテンツ配信におけるセキュリティ処理とコンテンツ蓄積の両方を MMC 110 によって容易に実現できる。コンテンツ料金の決済を、IC カードチップ 150 を利用して行ってもよい。

25 図 24 と図 25 は、それぞれ、本発明を SD カード（幅 24 ミリメートル、長さ 32 ミリメートル、厚さ 2.1 ミリメートルで、9 つの外部端子をもち、フラッシュメモリを搭載した小型メモリカードである。）とメモリースティック（メモリースティックはソニー株式会社の登録商標である。）に適用したときの簡単な内部構成図を表したものである。本発明を適用した SD カード 2410 は、S

Dカードコントローラチップ2420、フラッシュメモリチップ2430、SDカード外部端子2440、ICカードチップ150とを含む。本発明を適用したメモリースティック2510は、メモリースティックコントローラチップ2520、フラッシュメモリチップ2530、メモリースティック外部端子2540、ICカードチップ150とを含む。フラッシュメモリチップ2430と2530は、不揮発性の半導体メモリを記憶媒体とするメモリチップであり、フラッシュメモリコマンドによりデータの読み書きができる。SDカードコントローラチップ2420とメモリースティックコントローラチップ2520はそれぞれSDカードとメモリースティック内の他の構成要素を制御するマイコンチップである。

10 SDカード外部端子2440は9つの端子からなり、それらの位置は、端からData2端子2441、Data3端子2442、Com端子2443、Vss端子2444、Vdd端子2445、Clock端子2446、Vss端子2447、Data0端子2448、Data1端子2449の順で並んでいる。Vdd端子2445は電源供給端子、Vss端子2444と2447はグランド

15 端子、Data0端子2448とData1端子2449とData2端子2441とData3端子2442はデータ入出力端子、Com端子2443はコマンド入出力端子、Clock端子2446はクロック入力端子である。SDカード2410は、外部に接続するSDカードホスト機器2460とのインタフェース仕様にMMC110と違いがあるものの、MMC外部端子140と非常に類似

20 した外部端子を持ち、MMC110と同様に外部からコマンドを発行することにより動作する特徴を持つため、本発明を適用することができる。

一方、メモリースティック外部端子2540は10個の端子からなり、それらの位置は、端からGnd端子2541、BS端子2542、Vcc端子2543、予約端子Rsvを1つ飛ばしてDIO端子2544、INS端子2545、予約

25 端子Rsvを1つ飛ばしてSCK端子2546、Vcc端子2547、Gnd端子2548の順で並んでいる。Vcc端子2543と2547は電源供給端子、Gnd端子2541と2548はグランド端子、DIO端子2544はコマンドおよびデータ入出力端子、SCK端子2546はクロック入力端子である。メモリースティック2510は、外部に接続するメモリースティックホスト機器25

60とのインタフェース仕様にMMC110と違いがあるものの、MMC110と同様に外部からコマンドを発行することにより動作する特徴を持つため、本発明を適用することができる。

図1は、本発明を適用したMMCの詳細な内部構成図を表したものである。また、図2は、図1のMMC110と接続したホスト機器220の構成とその接続状態を表したものである。ホスト機器220は、VCC1電源221、CLK1発振器222、ホストインタフェース223を持つ。

MMC110は、外部のホスト機器220と情報交換するためのMMC外部端子140を持つ。MMC外部端子140は、CS端子141、CMD端子142、GND1端子143および146、VCC1端子144、CLK1端子145、DAT端子147の7つの端子とを含む。Multi Media Card仕様は、MMCの動作モードとしてMMCモードとSPIモードという2種類を規定しており、動作モードによってMMC外部端子140の使用法は異なる。本実施例ではMMCモードでの動作の場合について詳細に説明する。VCC1端子144は、VCC1電源221と接続されており、ホスト機器220がMMC110に電力を供給するための電源端子である。GND1端子143および146は、VCC1電源221と接続されており、MMC110の電氣的なグランド端子である。GND1端子143とGND1端子146は、MMC110内部で電氣的に短絡されている。CS端子141は、ホストインタフェース223に接続されており、SPIモードの動作において使用される入力端子である。ホスト機器220が、MMC110にSPIモードでアクセスするときには、CS端子141にLレベルを入力する。MMCモードの動作では、CS端子141を使用する必要はない。CMD端子142は、ホストインタフェース223に接続されており、ホスト機器220が、メモ리카ードインタフェース仕様に準拠したメモ리카ードコマンドをMMC110に送信したり、同仕様に準拠したメモ리카ードレスポンスをMMC110から受信するために使用する入出力端子である。DAT端子147は、ホストインタフェース223に接続されており、ホスト機器220が、メモ리카ードインタフェース仕様に準拠した形式の入力データをMMC110に送信したり、同仕様に準拠した形式の出力データをMMC110から受信するた

- めに使用する入出力端子である。CLK1端子145は、CLK1発振器222に接続されており、CLK1発振器222が生成するクロック信号が入力される端子である。ホスト機器220が、CMD端子142を通してメモリカードコマンド、メモリカードレスポンスを送受信したり、DAT端子147を通してホストデータを送受信するときに、CLK1端子145にクロック信号が入力される。ホストインタフェース223には、CLK1発振器222からクロック信号が供給されており、メモリカードコマンド、メモリカードレスポンス、ホストデータは、CLK1発振器222が生成するクロック信号にビット単位で同期して、ホスト機器220とMMC110との間を転送される。
- 10 MMC110は、コントローラチップ120を持つ。コントローラチップ120は、CPU121、フラッシュメモリI/F制御回路122、MMC I/F制御回路123、CLK0発振器124、VCC2生成器125、VCC2制御回路126、CLK2制御回路127、ICカードI/F制御回路128とを含む。これらの構成要素121～128は、ホスト機器220からVCC1端子144
- 15 やGND1端子143、146を通して供給された電力により動作する。MMC I/F制御回路123は、CS端子141、CMD端子142、CLK1端子145、DAT端子147と接続されており、MMC110がそれらの端子を通してホスト機器220と情報交換するためのインタフェースを制御する論理回路である。CPU121は、MMC I/F制御回路123と接続されており、MMC
- 20 I/F制御回路123を制御する。MMC I/F制御回路123がCMD端子142を通してホスト機器220からメモリカードコマンドを受信すると、MMC I/F制御回路123はそのコマンドの受信が成功したかどうかの結果をホスト機器220に伝えるためCMD端子142を通してホスト機器220にレスポンスを送信する。CPU121は、受信したメモリカードコマンドを解釈し、コマ
- 25 ンド内容に応じた処理を実行する。また、そのコマンド内容に応じてホスト機器220とDAT端子147を通してデータの送受信をおこなう必要がある場合、CPU121は、MMC I/F制御回路123へのデータの送出、MMC I/F制御回路123からのデータの取得をおこなう。さらに、CPU121は、MMC I/F制御回路123とホスト機器220との間のデータ転送手続きも制御す

る。例えば、ホスト機器 220 から受信したデータの処理中に、ホスト機器 220 が MMC 110 への電源供給を停止することがないように、CPU 121 は DAT 端子 147 に L レベルを出力させ、MMC 110 がビジー状態であることをホスト機器 220 に伝える。CLK0 発振器 124 は、CPU 121 と接続され、CPU 121 を動作させる駆動クロックを供給する。尚、IC カードチップ 150 は、駆動クロックを要するが、フラッシュメモリチップ 130 は、駆動クロックが不要である。しかし、IC カードチップ 150 及びフラッシュメモリチップ 130 は共に、データを転送するためのデータ転送クロックを要する。

MMC 110 は、フラッシュメモリチップ 130 を持つ。フラッシュメモリチップ 130 は、不揮発性の半導体メモリを記憶媒体とするメモリチップである。フラッシュメモリチップ 130 は、ホスト機器 220 から VCC1 端子 144 や GND1 端子 143、146 を通して供給された電力により動作する。フラッシュメモリチップ 130 は、外部からのフラッシュメモリコマンドに従って、入力されたデータを不揮発性の半導体メモリに格納するライト機能、また同メモリに格納されたデータを外部に出力するリード機能を持つ。フラッシュメモリ I/F 制御回路 122 は、フラッシュメモリチップ 130 にフラッシュメモリコマンドを発行したり、そのコマンドで入出力するデータを転送するための論理回路である。CPU 121 は、フラッシュメモリ I/F 制御回路 122 を制御し、フラッシュメモリチップ 130 にデータのライト機能やリード機能を実行させる。ホスト機器 220 から受信したデータをフラッシュメモリチップ 130 にライトしたり、フラッシュメモリチップ 130 に格納されたデータをホスト機器 220 に送信する必要があるとき、CPU 121 は、フラッシュメモリ I/F 制御回路 122 と MMC I/F 制御回路 123 の間のデータ転送を制御する。

MMC 110 は、IC カードチップ 150 を持つ。IC カードチップ 150 は、IC カードの基板中に埋め込むことを目的として設計された IC チップであり、IC カードの外部端子規格に準拠した 8 つの外部端子を持つ。このうち 6 つの端子は、IC カードの外部端子規格により使用法が割り付けられており、残りの 2 つは将来のための予備端子である。その 6 つの端子は、VCC2 端子 151、RST 端子 152、CLK2 端子 153、GND2 端子 155、VPP 端子 156、

I/O端子157である。

ICカードチップ150のグラント端子は、MMC外部端子140のGRN1
(グラント端子)146に接続される。ICカードチップ150のVCC2端子
(電源入力端子)151は、コントローラチップ120のVCC2制御回路12
5 6に接続される。ICカードチップ150のRST端子(リセット入力端子)1
52とI/O端子(データ入出力端子)157は、コントローラチップ120の
ICカードI/F制御回路128に接続される。ICカードチップ150のCLK
K2端子(クロック入力端子)153は、コントローラチップ120のCLK2
制御回路127に接続される。

10 フラッシュメモリチップ130のVCC端子(電源入力端子)は、MMC外部
端子140のVCC1144に接続される。フラッシュメモリチップ130のV
SS端子(グラント端子)は、MMC外部端子140のGRD1146に接続さ
れる。フラッシュメモリチップ130のI/O端子(データ入出力端子)とレデ
ィ/ビジー端子とチップイネーブル端子とアウトプットイネーブル端子とライト
15 イネーブル端子とクロック端子とリセット端子とは、コントローラチップ120
のフラッシュメモリIF制御回路122に接続される。

VCC2端子151は、ICカードチップ150に電力を供給するための電源
端子である。VCC2制御回路126は、MOS-FET素子を用いたスイッチ
回路によりVCC2端子151への電力の供給開始と供給停止を制御する回路で
20 ある。VCC2生成器125はVCC2端子151に供給する電圧を発生し、そ
れをVCC2制御回路126に供給する。ICカードの電気信号規格はICカー
ドの動作クラスとしてクラスAとクラスBを規定している。VCC2端子151
に供給する標準電圧は、クラスAでは5V、クラスBでは3Vである。本発明は
ICカードチップ150の動作クラスによらず適用できるが、本実施例ではIC
25 カードチップ150がクラスBで動作する場合について詳細に説明する。VPP
端子156は、ICカードチップ150がクラスAで動作する時に、内部の不揮
発性メモリにデータを書き込んだり消去したりするために使用される可変電圧を
供給する端子であり、クラスBで動作する時には使用しない。GND2端子15
5は、ICカードチップ150の電氣的なグラント端子であり、GND1端子1

4 3、1 4 6と短絡されている。VCC 2制御回路1 2 6はCPU 1 2 1と接続され、CPU 1 2 1はVCC 2端子1 5 1への電力供給の開始と停止を制御することができる。ICカードチップ1 5 0を使用しないときは、CPU 1 2 1はVCC 2端子1 5 1への電力供給を停止することができる。MMC 1 1 0は、IC
5 カードチップ1 5 0への電力供給を停止することにより、それが消費する電力を節約することができる。ただし、電力供給を停止すると、ICカードチップ1 5 0の内部状態は、ICカードチップ1 5 0内部の不揮発性メモリに記憶されたデータを除いて維持されない。

CLK 2端子1 5 3は、ICカードチップ1 5 0にクロック信号を入力する端子である。CLK 2制御回路1 2 7は、CLK 2端子1 5 3にクロックを供給する回路である。CLK 2制御回路1 2 7は、CLK 0発振器1 2 4から供給されたクロック信号をもとにしてCLK 2端子1 5 3に供給するクロック信号を生成する。CLK 2制御回路1 2 7はCPU 1 2 1と接続されており、CLK 2端子1 5 3へのクロックの供給開始と供給停止をCPU 1 2 1から制御することが
10 できる。ICカードチップ1 5 0は、自身内部に駆動クロック発振器をもたない。そのため、CLK 2端子1 5 3から駆動クロックを供給することによって動作する。CLK 2制御回路1 2 7が、CLK 2端子1 5 3へのクロック供給を停止すると、ICカードチップ1 5 0の動作は停止するため、ICカードチップ1 5 0の消費電力を低下させることができる。この時、VCC 2端子1 5 1への電力供給が保たれていれば、ICカードチップ1 5 0の内部状態は維持される。ここで、
15 CLK 2端子1 5 3に供給するクロック信号の周波数をF 2、CLK 0発振器1 2 4から供給されたクロック信号の周波数をF 0、PとQを正の整数とすると、CLK 2制御回路1 2 7は、 $F 2 = (P / Q) * F 0$ の関係になるようなクロック信号を作成して、これをCLK 2端子1 5 3に供給する。PとQの値はCPU
20 1 2 1により設定できるようになっている。Pを大きく設定してF 2を大きくすると、ICカードチップ1 5 0の内部処理をより高速に駆動できる。Qを大きく設定してF 2を小さくすると、ICカードチップ1 5 0の内部処理はより低速に駆動され、ICカードチップ1 5 0の消費電力を低下させることができる。ICカードチップ1 5 0の駆動クロック周波数は、ICカードチップ1 5 0が正しく

動作できるような許容周波数範囲内に設定される必要がある。そのため、CLK 2 制御回路 127 は、F 2 の値がその許容周波数範囲を外れるような P と Q の値を設定させない特徴を持つ。

I/O 端子 157 は、IC カードチップ 150 に IC カードコマンドを入力したり、IC カードチップ 150 が IC カードレスポンスを出力するときに使用する入出力端子である。IC カード I/F 制御回路 128 は、I/O 端子 157 と接続されており、I/O 端子 157 を通して IC カードコマンドの信号送信や IC カードレスポンスの信号受信をおこなう回路である。IC カード I/F 制御回路 128 は CPU 121 に接続されており、CPU 121 は、IC カード I/F 制御回路 128 による IC カードコマンドや IC カードレスポンスの送受信の手続きを制御したり、送信すべき IC カードコマンドデータを IC カード I/F 制御回路 128 に設定したり、受信した IC カードレスポンスを IC カード I/F 制御回路 128 から取得する。IC カード I/F 制御回路 128 には CLK 2 制御回路 127 からクロックが供給されており、IC カードコマンドや IC カードレスポンスは、CLK 2 端子 153 に供給するクロック信号にビット単位で同期して、I/O 端子 157 を通して送受信される。また、RST 端子 152 は、IC カードチップ 150 をリセットするときにリセット信号を入力する端子である。IC カード I/F 制御回路 128 は、RST 端子 152 と接続されており、CPU 121 の指示により IC カードチップ 150 にリセット信号を送ることができる。

IC カードチップ 150 は、IC カードの電気信号規格やコマンド規格に基づいて情報交換をおこなう。IC カードチップ 150 へのアクセスパターンは 4 種類であり、図 3～図 6 を用いて各パターンを説明する。図 3 は、CPU 121 の指示により IC カードチップ 150 が非活性状態（電源が遮断されている状態）から起動して内部状態を初期化するプロセス（以下、コールドリセットと呼ぶ）において、IC カードチップ 150 の外部端子の信号波形をシンプルに表したものである。図 4 は、CPU 121 の指示により IC カードチップ 150 が活性状態（電源が供給されている状態）で内部状態を初期化するプロセス（以下、ウォームリセットと呼ぶ）において、IC カードチップ 150 の外部端子の信号波形

をシンプルに表したものである。図5は、CPU121の指示によりICカードチップ150にICカードコマンドを送信しICカードチップ150からICカードレスポンスを受信するプロセスにおいて、ICカードチップ150の外部端子の信号波形をシンプルに表したものである。図6は、CPU121の指示によりICカードチップ150を非活性状態にするプロセスにおいて、ICカードチップ150の外部端子の信号波形をシンプルに表したものである。図3～図6において、時間の方向は左から右にとっており、上の行から下の行に向かってVCC2端子151、RST端子152、CLK2端子153、I/O端子157で観測される信号を表す。また、破線はそれぞれの信号の基準（Lレベル）を表す。

図3を参照して、ICカードチップ150のコールドリセット操作を説明する。まず、ICカードI/F制御回路128はRST端子152をLレベルにする（301）。次に、VCC2制御回路126はVCC2端子への電源供給を開始する（302）。次に、CLK2制御回路127はCLK2端子153へのクロック信号の供給を開始する（303）。次に、ICカードI/F制御回路128はI/O端子157を状態Z（プルアップされた状態）にする（304）。次に、ICカードI/F制御回路128はRST端子152をHレベルにする（305）。次に、ICカードI/F制御回路128はI/O端子157から出力されるリセット応答の受信を開始する（306）。リセット応答の受信が終了したら、CLK2制御回路127はCLK2端子153へのクロック信号の供給を停止する（307）。これで、コールドリセットの操作が完了する。なお、ステップ307は消費電力を低下させるための工夫であり、省略してもよい。

図4を参照して、ICカードチップ150のウォームリセット操作を説明する。まず、CLK2制御回路127はCLK2端子153へのクロック信号の供給を開始する（401）。次に、ICカードI/F制御回路128はRST端子152をLレベルにする（402）。次に、ICカードI/F制御回路128はI/O端子157を状態Zにする（403）。次に、ICカードI/F制御回路128はRST端子152をHレベルにする（404）。次に、ICカードI/F制御回路128はI/O端子157から出力されるリセット応答の受信を開始する（405）。リセット応答の受信が終了したら、CLK2制御回路127はCL

K 2 端子 1 5 3 へのクロック信号の供給を停止する (4 0 6)。これで、ウォームリセットの操作が完了する。なお、ステップ 4 0 6 は消費電力を低下させるための工夫であり、省略してもよい。

図 5 を参照して、I C カードチップ 1 5 0 に I C カードコマンドを送信し I C
5 カードチップ 1 5 0 から I C カードレスポンスを受信する操作を説明する。まず、
C L K 2 制御回路 1 2 7 は C L K 2 端子 1 5 3 へのクロック信号の供給を開始する (5 0 1)。なお、クロックがすでに供給されている場合、ステップ 5 0 1 は不要である。次に、I C カード I / F 制御回路 1 2 8 は I / O 端子 1 5 7 にコマンドデータの送信を開始する (5 0 2)。コマンドデータの送信が終了したら、
10 I C カード I / F 制御回路 1 2 8 は I / O 端子 1 5 7 を状態 Z にする (5 0 3)。次に、I C カード I / F 制御回路 1 2 8 は I / O 端子 1 5 7 から出力されるレスポンスデータの受信を開始する (5 0 4)。レスポンスデータの受信が終了したら、C L K 2 制御回路 1 2 7 は C L K 2 端子 1 5 3 へのクロック信号の供給を停止する (5 0 5)。これで、I C カードコマンド送信と I C カードレスポンス受
15 信の操作が完了する。なお、ステップ 5 0 5 は、消費電力を低下させるための工夫であり、省略してもよい。

図 6 を参照して、I C カードチップ 1 5 0 を非活性化する操作を説明する。まず、C L K 2 制御回路 1 2 7 は C L K 2 端子 1 5 3 を L レベルにする (6 0 1)。次に、I C カード I / F 制御回路 1 2 8 は R S T 端子 1 5 2 を L レベルにする
20 (6 0 2)。次に、I C カード I / F 制御回路 1 2 8 は I / O 端子 1 5 7 を L レベルにする (6 0 3)。最後に、V C C 2 制御回路 1 2 6 は V C C 2 端子への電源供給を停止する (6 0 4)。これで、非活性化の操作が完了する。

尚、I C カードチップ 1 5 0 の停止時 (例えば、セキュリティ処理を実行していない状態等) は、コントローラチップ 1 2 0 から I C カードチップ 1 5 0 へ電
25 源の供給を維持したまま、クロックの供給のみを停止してもよい。

I C カードチップ 1 5 0 は、機密データ保護や個人認証などに必要な暗号演算をおこなうセキュリティ処理機能を持つ。I C カードチップ 1 5 0 は、C P U 1 2 1 との間で I C カードコマンドや I C カードレスポンスの送受信することにより情報交換をおこない、その結果として、計算の結果や記憶されている情報の送

出、記憶されている情報の変更などをおこなう。CPU121は、ICカードチップ150を利用してセキュリティ処理を実行することができる。MMC110がホスト機器220から特定のメモ리카ードコマンドを受信すると、CPU121はそれを契機として、VCC2制御回路126を通してICカードチップ150への電源供給を制御したり、またはCLK2制御回路127を通してICカードチップ150へのクロック供給を制御したり、またはICカードI/F制御回路128を通してICカードチップ150にICカードコマンドを送信する。これにより、CPU121は、ICカードチップ150を利用して、ホスト機器220が要求するセキュリティ処理を実行する。CPU121は、特定のメモ리카ードコマンドの受信を契機に、ICカードチップ150に対する電源供給制御、クロック供給制御、ICカードコマンド送信、ICカードレスポンス受信を複数組み合わせて操作することによって、セキュリティ処理を実行してもよい。また、CPU121は、ホスト機器220がMMC110へ電源供給を開始したのを契機として、セキュリティ処理を実行してもよい。セキュリティ処理の結果は、ICカードチップ150が出力するICカードレスポンスをベースにして構成され、MMC110内に保持される。MMC110がホスト機器220から特定のメモ리카ードコマンドを受信すると、CPU121はそれを契機として、セキュリティ処理の結果をホスト機器220に送信する。

図7は、ホスト機器220がMMC110にアクセスするときのフローチャートを表したものである。まず、ホスト機器220はMMC110を活性化するためにVCC1端子144に電源供給を開始する(701)。これを契機として、MMC110は、第1次ICカード初期化処理を実行する(702)。第1次ICカード初期化処理の詳細は後述する。次に、ホスト機器220はMMC110を初期化するためにCMD端子142を通してMMC110の初期化コマンドを送信する(703)。この初期化コマンドはMulti Media Card仕様に準拠したものであり、複数種類ある。ホスト機器220は、MMC110を初期化するために、複数の初期化コマンドを送信する場合がある。MMC110が初期化コマンドを受信すると、MMC110はそれを処理する(704)。これを契機として、MMC110は、第2次ICカード初期化処理を実行する

(705)。第2次ICカード初期化処理の詳細は後述する。ホスト機器220は、MMC110の初期化コマンドに対するメモリカードレスポンスを、CMD端子142を通して受信し、そのメモリカードレスポンスの内容からMMC110の初期化が完了したかを判定する。未完了ならば、再び初期化コマンドの送信をおこなう(703)。MMC110の初期化が完了したならば、ホスト機器220は、Multi Media Card仕様に準拠した標準メモリカードコマンド(フラッシュメモリチップ130へアクセスするためのコマンド)や、上に述べたセキュリティ処理に関連した特定のメモリカードコマンド(ICカードチップ150へアクセスするためのコマンド)の送信を待機する状態に移る(707)。この待機状態では、ホスト機器220は標準メモリカードコマンドを送信することができる(708)。MMC110が標準メモリカードコマンドを受信したら、MMC110はそれを処理する(709)。処理が完了したら、ホスト機器220は、再び待機状態にもどる(707)。この待機状態では、ホスト機器220はセキュリティ処理要求ライトコマンドを送信することもできる(710)。セキュリティ処理要求ライトコマンドとは、上に述べたセキュリティ処理に関連した特定のメモリカードコマンドの1種であり、MMC110にセキュリティ処理を実行させるために処理要求を送信するメモリカードコマンドである。MMC110がセキュリティ処理要求ライトコマンドを受信したら、CPU121は、要求されたセキュリティ処理の内容を解釈し、セキュリティ処理をICカードコマンドの形式で記述する(711)。即ち、CPU121は、予め定められたルールに従って、ホスト機器230からの標準メモリカードコマンドを、ICカードチップ150が解釈可能な特定のメモリカードコマンドへ変換する。そして、その結果として得られたICカードコマンドをICカードチップ150に発行するなどして、要求されたセキュリティ処理を実行する(712)。処理が完了したら、ホスト機器220は、再び待機状態にもどる(707)。この待機状態では、ホスト機器220はセキュリティ処理結果リードコマンドを送信することもできる(713)。セキュリティ処理結果リードコマンドとは、上に述べたセキュリティ処理に関連した特定のメモリカードコマンドの1種であり、MMC110によるセキュリティ処理の実行結果を知るために処理結果を受信するメ

モリカードコマンドである。MMC 110がセキュリティ処理結果リードコマンドを受信したら、CPU 121は、ICカードチップ150から受信したICカードレスポンスをベースに、ホスト機器220に送信すべきセキュリティ処理結果を構築する(714)。そして、ホスト機器220は、MMC 110からセキュリティ処理結果を受信する。受信が完了したら、ホスト機器220は、再び待機状態にもどる(707)。なお、ステップ714は、ステップ712の中でおこなってもよい。

図7において、ステップ702およびステップ705で実行する第1次ICカード初期化処理および第2次ICカード初期化処理は、MMC 110内でセキュリティ処理を実行するのに備えて、CPU 121がICカードチップ150に対してアクセスする処理である。具体的には、ICカードチップ150の活性化や非活性化、ICカードチップ150のリセット、ICカードチップ150の環境設定を行う。環境設定とは、セキュリティ処理を実行するために必要な情報(例えば、使用可能な暗号アルゴリズムの情報、暗号計算に使用する秘密鍵や公開鍵に関する情報、個人認証に使用する認証データに関する情報など)をICカードチップ150から読み出したり、あるいはICカードチップ150に書き込んだりすることを意味する。ICカードチップ150の環境設定は、ICカードチップ150にICカードコマンドをN個(Nは正の整数)発行することによっておこなう。例えば、セッション鍵が3個必要ならば、ICカードコマンドを3回発行し、セッション鍵が2個必要ならば、ICカードコマンドを2回発行する。N個のICカードコマンドは、互いに相違するものであってもよいし、同一のものであってもよい。Nの値は固定されたものではなく、状況によってさまざまな値となる。以下、環境設定で発行するICカードコマンドを、設定コマンドと呼ぶ。また、この環境設定に基づいてセキュリティ処理を実行するICカードコマンドを、以下、セキュリティコマンドと呼ぶ。セキュリティコマンドの例としては、デジタル署名の計算、デジタル署名の検証、メッセージの暗号化、暗号化メッセージの復号、パスワードによる認証などをおこなうコマンドがある。

CPU 121は、ICカードチップ150の環境設定の内容を自由に変更することができる。CPU 121は、セキュリティ処理の内容や結果に応じてこれを

変更してもよいし、ホスト機器からのメモリカードコマンドの受信を契機としてこれを変更してもよい。また、CPU 121は、環境設定の内容を示した情報をフラッシュメモリチップ130にライトし、必要なときにフラッシュメモリチップ130からその情報をリードして使用することもできる。この情報は、図21
5 においてICカード環境設定情報2112として示されている。これにより、MMC 110が非活性化されてもその情報を保持することができ、MMC 110が活性化されるたびにあらためて設定する手間を省くことができる。

第1次ICカード初期化处理および第2次ICカード初期化处理は、ICカード制御パラメータA、B、Cに設定された値に基づいておこなわれる。また、C
10 PU 121は、ステップ712で実行するセキュリティ処理において、ICカード制御パラメータDに設定された値に基づいてICカードチップ150の活性化や非活性化を制御する。図8は、ICカード制御パラメータの種類と設定値、それに対応した処理の内容を表している。まず、パラメータAは、MMC 110に電源が供給されたときに実行される第1次ICカード初期化处理に関するパラメータである。A=0のときは、CPU 121はICカードチップ150にアクセスしない。A=1のときは、CPU 121はICカードチップ150をコールドリセットする。A=2のときは、CPU 121はICカードチップ150をコールドリセットした後でICカードチップ150の環境設定をおこなう。A=3の
15 ときは、CPU 121はICカードチップ150をコールドリセットした後でICカードチップ150の環境設定をおこない、最後にICカードチップ150を非活性化する。A=0またはA=3のときは、第1次ICカード初期化处理のあとICカードチップ150が非活性状態となる。A=1またはA=2のときは、第1次ICカード初期化处理のあとICカードチップ150は活性状態となる。次に、パラメータBとCは、MMC 110がMMC初期化コマンドを処理したと
20 きに実行される第2次ICカード初期化处理に関するパラメータである。B=0のときは、CPU 121はICカードチップ150にアクセスしない。B=1かつC=1のときは、CPU 121はICカードチップ150をリセット（コールドリセットまたはウォームリセット）する。B=1かつC=2のときは、CPU 121はICカードチップ150をリセットした後でICカードチップ150の

環境設定をおこなう。B=1かつC=3のときは、CPU121はICカードチップ150をリセットした後でICカードチップ150の環境設定をおこない、最後にICカードチップ150を非活性化する。B=2かつC=2のときは、CPU121はICカードチップ150の環境設定をおこなう。B=2かつC=3
5 のときは、CPU121はICカードチップ150の環境設定をおこなった後にICカードチップ150を非活性化する。B=3のときは、ICカードチップ150が活性状態ならば、CPU121はICカードチップ150を非活性化する。最後に、パラメータDは、ホスト機器220から要求されたセキュリティ処理を実行したあとに、ICカードチップ150を非活性化するか否かを示すパラメータである。D=0のときは、セキュリティ処理の実行後に、CPU121はIC
10 カードチップ150を非活性化せず、活性状態に保つ。D=1のときは、セキュリティ処理の実行後に、CPU121はICカードチップ150を非活性化する。

CPU121は、ICカード制御パラメータA、B、C、Dの設定値を変更することができる。CPU121は、セキュリティ処理の内容や結果に応じてこれ
15 らの設定値を変更してもよいし、ホスト機器からのメモリカードコマンドの受信を契機としてこれらの設定値を変更してもよい。また、CPU121は、これらの設定値をフラッシュメモリチップ130にライトし、必要なときにフラッシュメモリチップ130からこれらの設定値をリードして使用することもできる。これらの設定値は、図21においてICカード制御パラメータ2111として示さ
20 れている。これにより、MMC110が非活性化されてもこれらの設定値を保持することができ、MMC110が活性化されるたびにあらためて設定する手間を省くことができる。

図9は、第1次ICカード初期化処理のフローチャートを表している。初期化処理を開始する(901)と、まず、ICカード制御パラメータAが0かチェックする(902)。A=0ならばそのまま初期化処理は終了する(908)。A
25 =0でないならばICカードチップ150をコールドリセットする(903)。次に、ICカード制御パラメータAが1かチェックする(904)。A=1ならば初期化処理は終了する(908)。A=1でないならばICカードチップ150の環境設定をおこなう(905)。次に、ICカード制御パラメータAが2か

チェックする（９０６）。Ａ＝２ならば初期化処理は終了する（９０８）。Ａ＝２でないならばＩＣカードチップ１５０を非活性化する（９０７）。そして、初期化処理は終了する（９０８）。

図１０は、第２次ＩＣカード初期化処理のフローチャートを表している。初期
5 化処理を開始する（１００１）と、まず、ＩＣカード制御パラメータＢが０かチェックする（１００２）。Ｂ＝０ならばそのまま初期化処理は終了する（１０１３）。Ｂ＝０でないならばＢ＝１かチェックする（１００３）。Ｂ＝１ならばＩＣカード制御パラメータＡが０または３かチェックする（１００４）。Ａが０または３ならば、ＩＣカードチップ１５０をコールドリセットし（１００５）、ス
10 テップ１００７に移る。Ａが１または２ならば、ＩＣカードチップ１５０をウォームリセットし（１００６）、ステップ１００７に移る。ステップ１００７では、ＩＣカード制御パラメータＣが１かチェックする。Ｃ＝１ならば初期化処理は終了する（１０１３）。Ｃ＝１でないならばステップ１００９に移る。ステップ１
0 ０３においてＢ＝１でないならば、Ｂが２かチェックする（１００８）。Ｂ＝
15 ２ならばステップ１００９に移る。Ｂ＝２でないならば、ＩＣカード制御パラメータＡが０または３かチェックする（１０１１）。Ａが０または３ならば初期化処理を終了する（１０１３）。Ａが１または２ならば、ステップ１０１２に移る。ステップ１００９ではＩＣカードチップ１５０の環境設定をおこなう。そして、
ＩＣカード制御パラメータＣが２かチェックする（１０１０）。Ｃ＝２ならば初
20 期化処理を終了する（１０１３）。Ｃ＝２でないならばステップ１０１２に移る。ステップ１０１２ではＩＣカードチップ１５０を非活性化する。そして、初期化処理を終了する（１０１３）。

図１１は、ＩＣカードチップ１５０が非活性状態であるときに第１次ＩＣカード初期化処理あるいは第２次ＩＣカード初期化処理を実行した場合において、
25 ＩＣカードチップ１５０の外部端子の信号波形をシンプルに表したものである。図１２は、ＩＣカードチップ１５０が活性状態であるときに第２次ＩＣカード初期化処理を実行した場合において、ＩＣカードチップ１５０の外部端子の信号波形をシンプルに表したものである。図１１と図１２において、時間の方向は左から右にとっており、上の行から下の行に向かってＶＣＣ２端子１５１、ＲＳＴ端子

1 5 2、CLK 2 端子 1 5 3、I/O 端子 1 5 7 で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準（L レベル）を表す。図 1 1 において 1 1 0 2 は図 3 に示したコールドリセットの信号波形を表す。図 1 2 において 1 2 0 2 は図 4 に示したウォームリセットの信号波形を表す。図 1 1 と図 1 2 において、
5 第 1 設定コマンド処理 1 1 0 4 a と 1 2 0 4 a、第 2 設定コマンド処理 1 1 0 4 b と 1 2 0 4 b、第 N 設定コマンド処理 1 1 0 4 c と 1 2 0 4 c は、それぞれ図 5 に示した IC カードコマンド処理の信号波形を表す。IC カードチップ 1 5 0 の環境設定の信号波形 1 1 0 4 と 1 2 0 4 は、N 個の設定コマンド処理の信号波形が連なって構成される。図 1 1 と図 1 2 において、1 1 0 6 と 1 2 0 6 は、それぞれ図 6 に示した非活性化の信号波形を表す。図 1 1 と図 1 2 において、縦方向の破線 1 1 0 1、1 1 0 3、1 1 0 5、1 1 0 7、1 2 0 1、1 2 0 3、1 2 0 5、1 2 0 7 はそれぞれ特定の時刻を表す。1 1 0 1 はコールドリセット前の時刻、1 2 0 1 はウォームリセット前の時刻、1 1 0 3 はコールドリセット後から環境設定前の間にある時刻、1 2 0 3 はウォームリセット後から環境設定前の間にある時刻、1 1 0 5 と 1 2 0 5 は環境設定後から非活性化前の間にある時刻、1 1 0 7 と 1 2 0 7 は非活性化後の時刻である。

図 1 1 を参照して、第 1 次 IC カード初期化処理実行時の信号波形を示す。IC カード制御パラメータ A が 0 のときは、信号波形に変化はない。A = 1 のときは、時刻 1 1 0 1 から時刻 1 1 0 3 までの範囲の信号波形となる。A = 2 のときは、時刻 1 1 0 1 から時刻 1 1 0 5 までの範囲の信号波形となる。A = 3 のときは、時刻 1 1 0 1 から時刻 1 1 0 7 までの範囲の信号波形となる。

図 1 1 を参照して、IC カード制御パラメータ A が 0 または 3 のときの、第 2 次 IC カード初期化処理実行時の信号波形を示す。IC カード制御パラメータ B が 0 のときは、信号波形に変化はない。B = 1 かつ IC カード制御パラメータ C = 1 のときは、時刻 1 1 0 1 から時刻 1 1 0 3 までの範囲の信号波形となる。B = 1 かつ C = 2 のときは、時刻 1 1 0 1 から時刻 1 1 0 5 までの範囲の信号波形となる。B = 1 かつ C = 3 のときは、時刻 1 1 0 1 から時刻 1 1 0 7 までの範囲の信号波形となる。

図 1 2 を参照して、IC カード制御パラメータ A が 1 または 2 のときの、第 2

次 I C カード初期化処理実行時の信号波形を示す。I C カード制御パラメータ B が 0 のときは、信号波形に変化はない。B = 1 かつ I C カード制御パラメータ C = 1 のときは、時刻 1 2 0 1 から時刻 1 2 0 3 までの範囲の信号波形となる。B = 1 かつ C = 2 のときは、時刻 1 2 0 1 から時刻 1 2 0 5 までの範囲の信号波形となる。B = 1 かつ C = 3 のときは、時刻 1 2 0 1 から時刻 1 2 0 7 までの範囲の信号波形となる。B = 2 かつ C = 2 のときは、時刻 1 2 0 3 から時刻 1 2 0 5 までの範囲の信号波形となる。B = 2 かつ C = 3 のときは、時刻 1 2 0 3 から時刻 1 2 0 7 までの範囲の信号波形となる。B = 3 のときは、時刻 1 2 0 5 から時刻 1 2 0 7 までの範囲の信号波形となる。

- 10 図 1 3 は、図 7 のステップ 7 1 2 において、CPU 1 2 1 が、ホスト機器 2 2 0 が要求したセキュリティ処理を I C カードチップ 1 5 0 によって実行するときのフローチャートを表している。セキュリティ処理を開始する (1 3 0 1) と、まず I C カードチップ 1 5 0 が非活性状態かをチェックする (1 3 0 2)。非活性状態ならば、I C カードチップ 1 5 0 をコールドリセットし (1 3 0 3)、ステップ 1 3 0 6 に移る。活性状態ならば、ステップ 1 3 0 4 に移る。ステップ 1 3 0 4 では、I C カードチップ 1 5 0 に I C カードコマンドを発行する前に I C カードチップ 1 5 0 を再リセットする必要があるかをチェックする。必要があるならば、I C カードチップ 1 5 0 をウォームリセットし (1 3 0 5)、ステップ 1 3 0 6 に移る。必要がないならば、ステップ 1 3 0 6 に移る。ステップ 1 3 0 6 では、I C カードチップ 1 5 0 の環境設定をおこなう必要があるかをチェックする。必要があるならば、I C カードチップ 1 5 0 の環境設定をおこない (1 3 0 7)、ステップ 1 3 0 8 に移る。必要がないならば、ステップ 1 3 0 8 に移る。ステップ 1 3 0 8 では、I C カードチップ 1 5 0 の CLK 2 端子に供給するクロック信号の周波数 F 2 を設定する。そして、CPU 1 2 1 は I C カードチップ 1 5 0 にセキュリティコマンドを発行し、I C カードチップ 1 5 0 はそれを処理する (1 3 0 9)。セキュリティコマンドの処理時間は、クロック周波数 F 2 に依存する。次に、I C カードチップ 1 5 0 が出力する I C カードレスポンスにより、その処理が成功したかどうかを判定する (1 3 1 0)。成功ならば、ステップ 1 3 1 1 に移る。失敗ならば、ステップ 1 3 1 2 に移る。ステップ 1 3 1 1 では、

ICカードチップ150に発行すべきセキュリティコマンドが全て完了したかを
チェックする。発行すべきセキュリティコマンドがまだあるならば、ステップ1
304に移る。発行すべきセキュリティコマンドが全て完了したならば、ステッ
プ1314に移る。ステップ1312では、失敗したセキュリティコマンドをリ
5 トライすることが可能かを判定する。リトライできるなら、リトライ設定をおこ
ない(1313)、ステップ1304に移る。リトライ設定とは、リトライすべ
きセキュリティコマンドやその関連データをCPU121が再度準備すること
である。リトライできないならステップ1314に移る。これは、ホスト機器22
0が要求したセキュリティ処理が失敗したことを意味する。ステップ1314で
10 は、ICカード制御パラメータDをチェックする。D=1ならば、ICカードチ
ップ150を非活性化して(1315)、セキュリティ処理を終了する(131
6)。D=1でないならば、ICカードチップ150を活性状態に保ったままセ
キュリティ処理を終了する(1316)。図13のフローチャートにおいては、
クロック周波数F2を、ステップ1309で発行するセキュリティコマンドの種
15 類によって変えることができるように、ステップ1308をステップ1309の
直前に位置させたが、ステップ1308はそれ以外の位置にあってもよい。

従来のICカードへの攻撃法を有効にしている要因のひとつとして、ICカー
ドの駆動クロックが外部の接続装置から直接供給されることがあげられる。駆動
クロックが接続装置の制御下にあるため、タイミング解析や電力差分解析におい
20 ては、電気信号の測定においてICカード内部処理のタイミングの獲得が容易に
なる。一方、故障利用解析においては、異常な駆動クロックの供給による演算エ
ラーの発生が容易になる。これに対し、本発明によれば、MMC110内部でI
Cカードチップ150によりセキュリティ処理を実行するとき、ホスト機器22
0はICカードチップ150の駆動クロックを直接供給できない。CPU121
25 は、ICカードチップ150へ供給するクロックの周波数F2を自由に設定する
ことができる。これにより、ホスト機器220の要求する処理性能に柔軟に対応
したセキュリティ処理が実現できる。ホスト機器220が高速なセキュリティ処
理を要求するならば周波数F2を高く設定し、低い消費電力を要求するならば周
波数F2を低く設定したり、クロックを適度に停止させればよい。また、CPU

- 1 2 1は、周波数F 2だけでなくクロックの供給開始タイミング、供給停止タイミングを自由に設定できる。これらをランダムに変化させることにより、ICカードチップ1 5 0に対するタイミング解析、電力差分析、故障利用解析と呼ばれる攻撃法を困難にすることができる。タイミング解析は、攻撃者が暗号処理1 5 回の処理時間を正確に計測可能であることを仮定しているため、その対策としては、攻撃者が処理時間計測を正確に行えないようにすることが有効である。本発明によりタイミング解析が困難になる理由は、ICカードチップ1 5 0がICカードコマンドを処理している時間の長さをホスト機器2 2 0が正確に計測できないためである。電力差分析の対策としては、処理の実行タイミングや順序に関する情報を外部から検出不可能にすることが有効である。本発明により電力差分析が困難になる理由は、ICカードコマンドが発行された時刻、発行されたICカードコマンドの内容、発行されたICカードコマンドの順序（ICカードコマンドを複数組み合わせさせてセキュリティ処理を実行する場合）の検出がホスト機器2 2 0にとって困難になるためである。故障利用解析の対策としては、ICカードにクロックや電圧や温度等の動作環境検知回路を搭載し、異常を検出したならば処理を停止あるいは使用不能にするという方法が有効である。本発明により故障利用解析が困難になる理由は、CLK 2制御回路1 2 7がICカードチップ1 5 0に異常な駆動クロックを供給しないことが、ホスト機器2 2 0がICカードチップ1 5 0に演算エラーを発生させるのを防止するからである。
- 20 CPU 1 2 1は、ICカードチップ1 5 0に供給するクロックの周波数F 2、供給開始タイミング、供給停止タイミングの設定値を、セキュリティ処理の内容や結果に応じて変更してもよいし、ホスト機器からのメモリカードコマンドの受信を契機として変更してもよい。また、CPU 1 2 1は、これらの設定値をフラッシュメモリチップ1 3 0にライトし、必要なときにフラッシュメモリチップ1 3 0からこれらの設定値をリードして使用することもできる。これらの設定値は、図2 1においてCLK 2設定情報2 1 1 3として示されている。これにより、MMC 1 1 0が非活性化されてもこれらの設定値を保持することができ、MMC 1 1 0が活性化されるたびにあらためて設定する手間を省くことができる。

図1 4は、ホスト機器2 2 0がセキュリティ処理要求ライトコマンドをMMC

1 1 0に発行してから、I Cカードチップ1 5 0でセキュリティ処理が実行されるまでの過程（図7のステップ7 1 0～7 1 2）において、MMC 1 1 0およびI Cカードチップ1 5 0の外部端子の信号波形、C P U 1 2 1によるフラッシュメモリチップ1 3 0へのアクセスをシンプルに表したものである。図1 4において、時間の方向は左から右にとる。一番上の行はフラッシュメモリチップ1 3 0へのアクセス内容である。上から二行目の行から下の行に向かって、V C C 1 端子1 4 4、C M D 端子1 4 2、C L K 1 端子1 4 5、D A T 端子1 4 7、V C C 2 端子1 5 1、R S T 端子1 5 2、C L K 2 端子1 5 3、I / O 端子1 5 7で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準（L レベル）を表す。図1 4を参照して、ホスト機器2 2 0がセキュリティ処理要求ライトコマンドをMMC 1 1 0に発行してから、I Cカードチップ1 5 0でセキュリティ処理が実行されるまでの過程を説明する。まず、ホスト機器2 2 0はC M D 端子1 4 2にセキュリティ処理要求ライトコマンドを送信する（1 4 0 1）。次に、ホスト機器2 2 0はC M D 端子1 4 2からセキュリティ処理要求ライトコマンドのレスポンスを受信する（1 4 0 2）。このレスポンスは、MMC 1 1 0がコマンドを受信したことをホスト機器2 2 0に伝えるものであり、セキュリティ処理の実行結果ではない。次に、ホスト機器2 2 0はD A T 端子1 4 7にセキュリティ処理要求を送信する（1 4 0 3）。セキュリティ処理要求とは、セキュリティ処理の内容や処理すべきデータを含むホストデータである。次に、MMC 1 1 0はD A T 端子1 4 7をL レベルにセットする（1 4 0 4）。MMC 1 1 0は、これによりビジー状態であることをホスト機器2 2 0に示す。次に、C P U 1 2 1は、ホスト機器2 2 0から受信したセキュリティ処理要求をフラッシュメモリチップ1 3 0にライトするコマンドを発行する（1 4 0 5）。セキュリティ処理要求をフラッシュメモリチップ1 3 0にライトすることにより、C P U 1 2 1がセキュリティ処理要求をI Cカードコマンド形式で記述する処理（図7のステップ7 1 1）において、C P U 1 2 1内部のワークメモリの消費量を節約できる。これは、セキュリティ処理要求のデータサイズが大きいときに有効である。なお、フラッシュメモリチップ1 3 0にライトされたセキュリティ処理要求は、図2 1においてセキュリティ処理バッファ領域2 1 1 4に格納される。また、ライトコ

マンド発行1405は必須な操作ではない。ライト処理期間1406は、フラッシュメモリチップ130がセキュリティ処理要求のライト処理を実行している期間を表す。セキュリティ処理1407はICカードチップ150によるセキュリティ処理の信号波形を表す。この信号波形は図13のフローチャートの遷移過程5に依存する。セキュリティ処理1407は、ライト処理期間1406とオーバーラップさせることができる。一般にフラッシュメモリチップ130のライト処理期間1406はミリ秒のオーダーであるため、セキュリティ処理1407とオーバーラップさせることは、セキュリティ処理の全体的な処理時間の短縮にとって有効である。リード／ライト1408は、セキュリティ処理1407の実行中に、フラッシュメモリチップ130からセキュリティ処理要求をリードしたり、ICカードチップ150が出力した計算結果をフラッシュメモリチップ130にライトするアクセスを示している。このアクセスにより、CPU121内部のワークメモリの消費量を節約できる。これは、セキュリティ処理要求やセキュリティ処理結果のデータサイズが大きいときに有効である。リード／ライト1408は必須ではない。セキュリティ処理1407が完了したら、MMC110はDAT端子147をHレベルにセットする(1409)。MMC110は、これによりセキュリティ処理が完了したことをホスト機器220に示す。

図15は、図14におけるセキュリティ処理1407の信号波形の一例を表したものである。図15において、時間の方向は左から右にとる。一番上の行はフラッシュメモリチップ130へのアクセス内容である。上から二行目の行から下の行に向かって、VCC2端子151、RST端子152、CLK2端子153、I/O端子157で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準(Lレベル)を表す。1501は図3に示したコールドリセットの信号波形を表し、1504は図4に示したウォームリセットの信号波形を表し、1502および1505は図11(あるいは図12)に示した環境設定の信号波形を表し、1503および1506および1507は図5に示したICカードコマンド処理の信号波形を表し、1508は図6に示した非活性化の信号波形を表す。ICカードチップ150の外部端子において図15に示した信号波形が観測されるのは、図13のフローチャートが1301、1302、1303、1306、

1307、1308、1309、1310、1311、1304、1305、1306、1307、1308、1309、1310、1311、1304、1306、1308、1309、1310、1311、1314、1315、1316の順で遷移するときである。図15を参照して、図14のセキュリティ処理1407の実行中におけるCPU121によるフラッシュメモリチップ130へのアクセス（リード／ライト1408）を説明する。このアクセスには、図21におけるセキュリティ処理バッファ領域2114を使用する。リード1509、1511、1512は、それぞれ、セキュリティコマンド処理1503、1506、1507においてICカードチップ150に送信するICカードコマンドを構築するために必要なデータを、フラッシュメモリチップ130からリードするアクセスである。ライト1510は、セキュリティコマンド処理1503においてICカードチップ150が出力した計算結果を、フラッシュメモリチップ130にライトするアクセスである。ライト1513は、セキュリティコマンド処理1506および1507においてICカードチップ150が出力した計算結果を、フラッシュメモリチップ130にまとめてライトするアクセスである。リード1509、1511、1512は、それぞれ、セキュリティコマンド処理1503、1506、1507以前のICカードチップ150へのアクセスとオーバーラップさせることができる。ライト1510、1513は、それぞれ、セキュリティコマンド処理1503、1507以後のICカードチップ150へのアクセスとオーバーラップさせることができる。これらのオーバーラップは、セキュリティ処理の全体的な処理時間の短縮にとって有効である。さらに、フラッシュメモリチップ130のライト単位が大きい場合は、ライト1513のように複数の計算結果をまとめてライトすることができる。これは、フラッシュメモリチップ130へのライト回数を削減し、フラッシュメモリチップ130の劣化を遅らせる効果がある。なお、ライト1510、1513でフラッシュメモリチップ130にライトする内容は、ICカードチップ150が出力した計算結果そのものに限定されず、図7のステップ715でホスト機器220に返すセキュリティ処理結果またはその一部であってもよい。この場合、図7のステップ714またはその一部は、ステップ712の中で実行されることになる。

図16は、ホスト機器220がセキュリティ処理結果リードコマンドをMMC110に発行してから、MMC110がセキュリティ処理結果を出力するまでの過程（図7のステップ713～715）において、MMC110の外部端子の信号波形、CPU121によるフラッシュメモリチップ130へのアクセスをシン

5 プルに表したものである。図16において、時間の方向は左から右にとる。一番上の行はフラッシュメモリチップ130へのアクセス内容である。上から二行目の行から下の行に向かって、VCC1端子144、CMD端子142、CLK1端子145、DAT端子147で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準（Lレベル）を表す。図16を参照して、ホスト機器22

10 0がセキュリティ処理結果リードコマンドをMMC110に発行してから、MMC110がセキュリティ処理結果を出力するまでの過程を説明する。まず、ホスト機器220はCMD端子142にセキュリティ処理結果リードコマンドを送信する（1601）。次に、ホスト機器220はCMD端子142からセキュリティ処理結果リードコマンドのレスポンスを受信する（1602）。このレスポンスは、MMC110がコマンドを受信したことをホスト機器220に伝えるものであり、セキュリティ処理結果ではない。次に、MMC110はDAT端子147をLレベルにセットする（1603）。MMC110は、これによりビジー状態であることをホスト機器220に示す。次に、CPU121は、フラッシュメモリチップ130のセキュリティ処理バッファ領域（図21の2114）から、

20 ICカードチップ150が出力した計算結果をリードする（1604）。CPU121は、これをもとにセキュリティ処理結果を構築し、MMC110がDAT端子147にセキュリティ処理結果を出力する（1605）。なお、図7のステップ714またはその一部が、ステップ712の中で実行されている場合、ステップ1604ではフラッシュメモリチップ130のセキュリティ処理バッファ領域（図21の2114）からセキュリティ処理結果またはその一部をリードする。

25 域（図21の2114）からセキュリティ処理結果またはその一部をリードする。なお、フラッシュメモリチップ130のセキュリティ処理バッファ領域（図21の2114）を利用しないでセキュリティ処理結果を構築する場合、ステップ1604は必要ない。

図27は、図7のステップ710においてMMC110に送信するセキュリテ

ィ処理要求データ、およびステップ715でホスト機器220が受信するセキュリティ処理結果データそれぞれのフォーマットの一例を示したものである。このフォーマットは、要求されたセキュリティ処理の内容が1つのICカードコマンドで表現でき、セキュリティ処理の結果が1つのICカードレスポンスで表現できる場合に適用することが好ましい。ICカードチップ150に送信するICカードコマンド、ICカードチップ150から受信するICカードレスポンスはともにISO/IEC7816-4規格に従う。本規格によれば、ICカードコマンドの構成は、4バイトのヘッダ（クラスバイトCLA、命令バイトINS、パラメータバイトP1とP2）が必須であり、必要に応じて、入力データ長指示バイトLc、入力データData In、出力データ長指示バイトLeが後に続く。

また、ICカードレスポンスの構成は、2バイトのステータスSW1とSW2が必須であり、必要に応じて、出力データData Outがその前に置かれる。本フォーマットにおけるセキュリティ処理要求のデータ2701は、ICカードコマンド2702の前にフォーマット識別子FID2703とICカードコマンド長Lca2704を付け、さらにICカードコマンド2702の後にダミーデータ2705をパディングしたものである。FID2703はフォーマットの識別番号またはフォーマットの属性データを含む。Lca2704の値はICカードコマンド2702の各構成要素の長さを合計した値である。一方、セキュリティ処理結果のデータ2711は、ICカードレスポンス2712の前にフォーマット識別子FID2713とICカードレスポンス長Lra2714を付け、さらにICカードレスポンス2712の後にダミーデータ2715をパディングしたものである。FID2713はフォーマットの識別番号またはフォーマットの属性データを含む。Lra2714の値はICカードレスポンス2712の各構成要素の長さを合計した値である。なお、この図では、ICカードコマンドにLc、Data In、Leが含まれ、ICカードレスポンスにData Outが含まれる場合のフォーマット例を表している。Multi Media Card仕様では、リード/ライトアクセスするデータを固定長のブロック単位で処理することが標準となっている。よって、セキュリティ処理要求のデータ2701やセキュリティ処理結果のデータ2711のサイズもMulti

Media Card仕様に準拠したブロックサイズに一致させることが好ましい。ダミーデータ2705、2715は、セキュリティ処理要求のデータ2701やセキュリティ処理結果のデータ2711のサイズをブロックサイズに一致させるために適用される。ブロックサイズとして採用する値は、一般の小型メモリ
5 カードが論理ファイルシステムに採用しているFAT方式におけるセクタサイズ（512バイト）が望ましい。パディングするダミーデータ2705、2715は全てゼロでもよいし、乱数でもよいし、CPU121やホスト機器220がデータエラーを検出したり訂正するためのチェックサムでもよい。Lca2704の値はCPU121がセキュリティ処理要求のデータ2701からダミーデータ
10 2705を除去するために使用し、Lra2714の値はホスト機器220がセキュリティ処理結果のデータ2711からダミーデータ2715を除去するために使用する。

MMC110の製造者や管理者は、セキュリティシステムのユーザにMMC110を提供する前やそのユーザが所有するMMC110に問題が発生した時に、
15 MMC110に内蔵されたICカードチップ150に様々な初期データを書きこんだり、ICカードチップ150のテストをおこなったりする必要がある。MMC110の製造者や管理者によるこれらの操作の利便性を高めるために、MMC110は、ICカードチップ150の外部端子をMMC外部端子140に割りつけるインタフェース機能を持つ。これにより、図3～図6で示したようなICカードチップ150へのアクセス信号を、MMC外部端子140から直接送受信で
20 きる。このようなMMC110の動作モードを、Multi Media Card仕様に準拠した動作モードと区別して、以下、インタフェース直通モードと呼ぶ。

インタフェース直通モードについて詳細に説明する。図17は、ICカードチップ150の外部端子をMMC外部端子140に割りつけるときの対応関係の一例を表している。この例では、RST端子152をCS端子141に割り付け、GND2端子155をGND1端子143、146に割り付け、VCC2端子151をVCC1端子144に割り付け、CLK2端子153をCLK1端子145に割り付け、I/O端子157をDAT端子147に割り付ける。このとき、
25

CS端子141とCLK1端子145は入力端子、DAT端子147は入出力端子として機能する。

- MMC110は、特定のメモ리카ードコマンドを受信すると、動作モードをインタフェース直通モードへ移したり、インタフェース直通モードからMulti Media Card仕様に準拠した動作モードに戻ることができる。以下、動作モードをインタフェース直通モードへ移すメモ리카ードコマンドを直通化コマンド、動作モードをインタフェース直通モードから通常の状態に戻すメモ리카ードコマンドを復帰コマンドと呼ぶ。図1を参照して、MMC I/F制御回路123は、VCC2制御回路126、CLK2制御回路127、ICカードI/F制御回路128と接続されており、MMC110がホスト機器220から直通化コマンドを受信すると、CPU121の指示により図17で示した端子割り付けをおこなう。MMC110がホスト機器220から復帰コマンドを受信すると、CPU121の指示により図17で示した端子割り付けを解除し、MMC110はMulti Media Card仕様に準拠した動作モードに戻る。
- 15 インタフェース直通モードでは、ホスト機器220がICカードチップ150に直接アクセスできるため、セキュリティの観点からインタフェース直通モードを利用できるのは限られた者だけに必要がある。そこで、直通化コマンドの発行には、一般のユーザに知られないパスワードの送信を必要とする。正しいパスワードが入力されないとインタフェース直通モードは利用できない。
- 20 図18は、ホスト機器220が、MMC110の動作モードをMulti Media Card仕様に準拠した動作モードからインタフェース直通モードに移し、ICカードチップ150に直接アクセスし、その後、MMC110の動作モードを再びMulti Media Card仕様に準拠した動作モードに戻すまでの処理のフローチャートを表している。ホスト機器220は処理を開始
- 25 し(1801)、まずMMC110に直通化コマンドを発行する(1802)。MMC110は、直通化コマンドで送信されたパスワードが正しいかチェックする(1803)。正しければステップ1804に移り、間違っていれば処理は終了する(1810)。ステップ1804では、CPU121は、ICカードチップ150をコールドリセットする。そして、図17で示した端子割り付けをおこ

ないインタフェースを直通化する（1805）。この時点から、ホスト機器220はICカードチップ150に直接アクセスする（1806）。ホスト機器220がICカードチップ150への直接アクセスを終了し、MMC110の動作モードを再びMulti Media Card仕様に準拠した動作モードに戻すときは、MMC110に復帰コマンドを発行する（1807）。すると、CPU121は図17で示した端子割り付けを解除し、MMC110はMulti Media Card仕様に準拠した動作モードに戻る（1808）。そして、CPU121は、ICカードチップ150を非活性化する（1809）。以上で、処理は終了する（1810）。

10 図19は、図18のステップ1801～1806の過程において、MMC110およびICカードチップ150の外部端子の信号波形をシンプルに表したものである。図19において、時間の方向は左から右にとる。上の行から下の行に向かって、VCC1端子144、CMD端子142、CLK1端子145、DAT端子147、VCC2端子151、RST端子152、CLK2端子153、I/O端子157で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準（Lレベル）を表す。1905は、図3のコールドリセットの信号波形を示す。モード移行時刻1906は、動作モードがインタフェース直通モードに移る時刻を表す。

図19を参照して、ホスト機器220がMMC110の動作モードを
20 Multi Media Card仕様に準拠した動作モードからインタフェース直通モードに移しICカードチップ150に直接アクセスする過程を説明する。なお、MMC110のVCC1端子144には3V（VCC2端子151の標準電圧）が供給されている。ホスト機器220がCMD端子142に直通化コマンドを入力すると（1901）、CMD端子142から直通化コマンドのレスポンスが出力される（1902）。このレスポンスは、MMC110がコマンドを受信したことをホスト機器220に伝えるものである。次に、ホスト機器220はDAT端子147にパスワードを入力する（1903）。パスワード入力後、MMC110はDAT端子147にLレベルを出力し（1904）、ビジー状態であることをホスト機器220に示す。ビジー状態の間に、CPU121は、IC

カードチップ150をコールドリセットする(1905)。そして、モード移行時刻1906において、動作モードをインタフェース直通モードに移す。このときに、DAT端子147はLレベルからハイインピーダンス状態になる。これにより、ホスト機器220はビジー状態の解除を知ることができる。この時点から、

5 ホスト機器220はICカードチップ150に直接アクセスする。例えば、CLK1端子145にクロックを供給すると(1907)、CLK2端子153にそのクロックが供給される(1908)。また、DAT端子147にICカードコマンドを送信すると(1909)、I/O端子157にそのICカードコマンドが送信される(1910)。

- 10 図20は、図18のステップ1807~1810の過程において、MMC110およびICカードチップ150の外部端子の信号波形をシンプルに表したものである。図20において、時間の方向は左から右にとる。上の行から下の行に向かって、VCC1端子144、CMD端子142、CLK1端子145、DAT端子147、VCC2端子151、RST端子152、CLK2端子153、I/O端子157で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準(Lレベル)を表す。モード復帰時刻2003は、動作モードがインタフェース直通モードからMulti Media Card仕様に準拠した動作モードに戻る時刻を表す。2004は、図6の非活性化の信号波形を示す。
- 15

- 図20を参照して、ホスト機器220がMMC110の動作モードをインタフェース直通モードからMulti Media Card仕様に準拠した動作モードに戻す過程を説明する。なお、MMC110のVCC1端子144には3V(VCC2端子151の標準電圧)が供給されている。ホスト機器220がCMD端子142に復帰コマンドを入力すると(2001)、CMD端子142から復帰コマンドのレスポンスが出力される(2002)。このレスポンスは、MMC
- 20
- 25 C110がコマンドを受信したことをホスト機器220に伝えるものである。そして、モード復帰時刻2003において、MMC110はDAT端子147にLレベルを出力してビジー状態であることをホスト機器220に示し、それと同時に動作モードをMulti Media Card仕様に準拠した動作モードに戻る。ビジー状態の間に、CPU121は、ICカードチップ150を非活性化

する（２００４）。そして、MMC１１０は、DAT端子１４７をハイインピーダンス状態にし（２００５）、復帰コマンドの処理が完了したことをホスト機器２２０に示す。これ以後、ホスト機器２２０はＩＣカードチップ１５０に直接アクセスできない。ホスト機器２２０が、CLK１端子１４５にクロックを供給しながらCMD端子１４２に何らかのメモ리카ードコマンドを送信した場合、ＩＣカードチップ１５０にそのクロック信号（２００６）は伝わらない。２００１や２００２においてホスト機器２２０がCLK１端子１４５に供給するクロック信号は、ＩＣカードチップ１５０のCLK２端子１５３にも伝わるが、DAT端子１４７がハイインピーダンス状態であるため、ＩＣカードチップ１５０がＩＣカードコマンドを誤って認識することはない。

図２１において、セキュリティ処理ステータス領域２１１６には、ＩＣカードチップ１５０によるセキュリティ処理の進捗状況を示す情報を格納する。CPU１２１は、この情報をセキュリティ処理の実行中に更新することができる。例えば、セキュリティ処理の途中でMMC１１０への電源供給が停止した場合、電源供給再開時にCPU１２１がこの情報をリードして参照すれば、セキュリティ処理を中断した段階から再開することができる。

本発明の実施形態によれば、メモ리카ード外部からＩＣチップの駆動クロックを直接供給しないため、ＩＣチップの処理時間を正確に計測できず、また、処理の実行タイミングや順序の検出が困難になる。さらに、異常な駆動クロックを供給することができず、演算エラーを発生させるのが困難になる。したがって、タイミング解析、電力差分析、故障利用解析攻撃法に対するセキュリティが向上する。

本発明の実施形態によれば、メモ리카ード外部からＩＣチップの制御方式を自由に設定できる。例えば、高速処理が要求されるならば、ＩＣチップの駆動クロックの周波数を高くした制御方式を設定し、低消費電力が要求されるならば、ＩＣチップの駆動クロックの周波数を低くしたり、ＩＣチップの駆動クロックを適度に停止させる制御方式を設定することができる。したがって、セキュリティシステムの要求する処理性能に柔軟に対応したセキュリティ処理が実現できる。

本発明によれば、ＩＣチップによるセキュリティ処理に必要なデータや、ＩＣ

チップを管理するための情報を、フラッシュメモリに保持することができる。したがって、セキュリティ処理の利便性を向上させることができる。

本発明の実施形態によれば、MMCの製造者や管理者が、MMC内部のICチップに直接アクセスすることができる。したがって、MMC内部のICチップの初期化やメンテナンスを、従来のICカードと同様な方法で実現できる。

本発明の実施形態によれば、フラッシュメモリチップを備えたMMCに、セキュリティ機能を追加する場合、セキュリティ評価機関の認証を予め受けたICカードチップ追加搭載することによって、セキュリティ評価機関によるMMCの認証が不要となるため、MMCの開発期間又は製造期間が短縮する。

10 産業上の利用可能性

本発明によれば、記憶装置のセキュリティを向上するという効果を奏する。

本発明によれば、記憶装置の製造が簡略化されるという効果を奏する。

上記記載は実施例についてなされたが、本発明はその精神と添付クレームの範囲内で種々の変更および修正をすることができることは当業者に明らかである。

請求の範囲

1. データを記憶可能なフラッシュメモリチップと、前記フラッシュメモリチップへの前記データの読み書きを制御するコントローラとを備えたメモリカード
- 5 において、
認証機関によって予め認証された I C チップを備え、
前記コントローラは、前記 I C チップを制御可能であるメモリカード。
2. 請求の範囲第 1 項に記載のメモリカードにおいて、
前記 I C チップは、当該メモリカードが接続可能な外部のホスト機器からのコ
- 10 マンドを、前記コントローラを介して受信するメモリカード。
3. データを記憶するための記憶装置において、
前記データを記憶可能なメモリと、前記データを記憶可能でかつ前記データのセキュリティ処理を実行可能な処理装置と、外部のホスト機器からのコマンドに基づいて、前記メモリと前記処理装置とを制御するコントローラとを備えた記憶
- 15 装置。
4. 請求の範囲第 3 項に記載の記憶装置において、
前記コントローラは、前記ホスト機器からの前記コマンドに前記データのセキュリティ処理に関する情報が含まれていた場合に、前記処理装置を選択し制御する記憶装置。
- 20 5. 請求の範囲第 3 項に記載の記憶装置において、
前記データのセキュリティ処理は、前記データの暗号化又は復号化のための処理を含む記憶装置。
6. 請求の範囲第 3 項に記載の記憶装置において、
前記コントローラは、前記メモリが解釈可能な第 1 のコマンドを前記ホスト機
- 25 器から受信し、予め定められたルールに従って、前記第 1 のコマンドを、前記処理装置が解釈可能な第 2 のコマンドへ変換し、前記第 2 のコマンドを前記処理装置へ送信する記憶装置。
7. 請求の範囲第 3 項に記載の記憶装置において、
前記メモリは、前記コントローラが前記処理装置への前記データの書き込み要

求を前記ホスト機器から受信した場合に、前記データが前記処理装置へ書き込まれるためのバッファとして利用される記憶装置。

8. 請求の範囲第3項に記載の記憶装置において、

前記コントローラは、前記ホスト機器から書き込み要求されたデータのサイズ
5 に応じて、前記メモリをバイパスして前記処理装置に前記データを送信するか又は前記メモリに一旦記憶させた後に前記処理装置へ前記データを送信するかを決定する記憶装置。

9. 請求の範囲第8項に記載の記憶装置において、

前記コントローラは、前記ホスト機器から書き込み要求されたデータのサイズ
10 が、前記処理装置が受信可能な許容データサイズ以上の場合に、前記メモリに一旦記憶させた後に前記処理装置へ前記データを送信する記憶装置。

10. 請求の範囲第8項に記載の記憶装置において、

前記コントローラは、前記ホスト機器から書き込み要求されたデータのサイズ
15 が、前記処理装置が受信可能な許容データサイズ以下の場合に、前記メモリをバイパスして前記処理装置に前記データを送信する記憶装置。

11. 請求の範囲第3項に記載の記憶装置において、

前記メモリは、

前記ホスト機器からアクセス可能な第1の記憶領域と、

前記ホスト機器からのアクセスが制限され、かつ、前記コントローラと前記処
20 理装置の少なくとも1つからの要求に応じて、前記処理装置によって利用されるデータを記憶するための第2の領域とを備える記憶装置。

12. 請求の範囲第11項に記載の記憶装置において、

前記処理装置によって利用されるデータは、当該処理装置を制御するためのパラメータと、当該処理装置の環境設定のための情報と、当該処理装置を制御する
25 ためのクロックを設定するための情報と、当該処理装置がセキュリティ処理を実行するためのステータスとの、少なくとも1つを含む記憶装置。

13. 請求の範囲第3項に記載の記憶装置において、

前記コントローラは、前記処理装置を駆動するための駆動クロックを生成する記憶装置。

14. 請求の範囲第 1 3 項に記載の記憶装置において、
前記コントローラは、前記処理装置を駆動するための電力を生成する記憶装置。
15. 請求の範囲第 1 4 項に記載の記憶装置において、
前記コントローラは、前記処理装置を停止する場合に、前記処理装置への前記
- 5 電力の供給を維持したまま、前記処理装置への前記駆動クロックの供給を停止する記憶装置。
16. 請求の範囲第 1 3 項に記載の記憶装置において、
前記コントローラは、前記ホスト機器からの処理要求が低速である場合の前記
- 10 駆動クロックの周波数よりも、前記ホスト機器からの処理要求が高速である場合の前記駆動クロックの周波数を大きくする記憶装置。
17. 外部のホスト機器からのデータを記憶可能なフラッシュメモリチップと、
前記フラッシュメモリチップへの前記データの読み書きを制御するコントローラ
と、前記コントローラと前記ホスト機器とを接続するための外部端子とを備えた
メモリカードにおいて、
- 15 前記ホスト機器からのデータを処理し、記憶するための I C チップを備え、
前記 I C チップのグランド端子は、前記外部端子に接続され、
前記 I C チップの電源入力端子とリセット入力端子とクロック入力端子とデータ
入出力端子は、前記コントローラに接続されるメモリカード。
18. 請求の範囲第 1 7 項に記載のメモリカードにおいて、
- 20 前記フラッシュメモリチップの電源端子とグランド端子は、前記外部端子に接
続され、
前記フラッシュメモリチップのデータ入出力端子とレディ／ビジー端子とチッ
プイネーブル端子とアウトプットイネーブル端子とライトイネーブル端子とクロ
ック端子とリセット端子とは、前記コントローラに接続されるメモリカード。
- 25 19. 外部のホスト機器からのデータを記憶可能なメモリと、前記ホスト機器か
らの要求に応じて前記メモリへのアクセスを制御するコントローラとを備えた記
憶装置において、
前記ホスト機器からのデータを処理し、記憶する処理装置を備え、
前記コントローラは、前記処理装置への電源供給が停止している場合に、前記

処理装置への電源供給開始を指示し、その後、前記処理装置への前記処理装置を駆動するための駆動クロックの供給開始を指示し、その後、前記処理装置のデータ入出力端子をプルアップ状態とし、その後、前記処理装置へ供給するリセット信号をハイレベル状態とし、

- 5 前記コントローラは、前記処理装置へ電源が供給されている場合に、前記処理装置へ前記駆動クロック供給を停止し、前記リセット信号をローレベル状態とし、前記データ入出力端子をプルアップ状態とし、前記リセット信号をハイレベルとする記憶装置。

FIG. 1

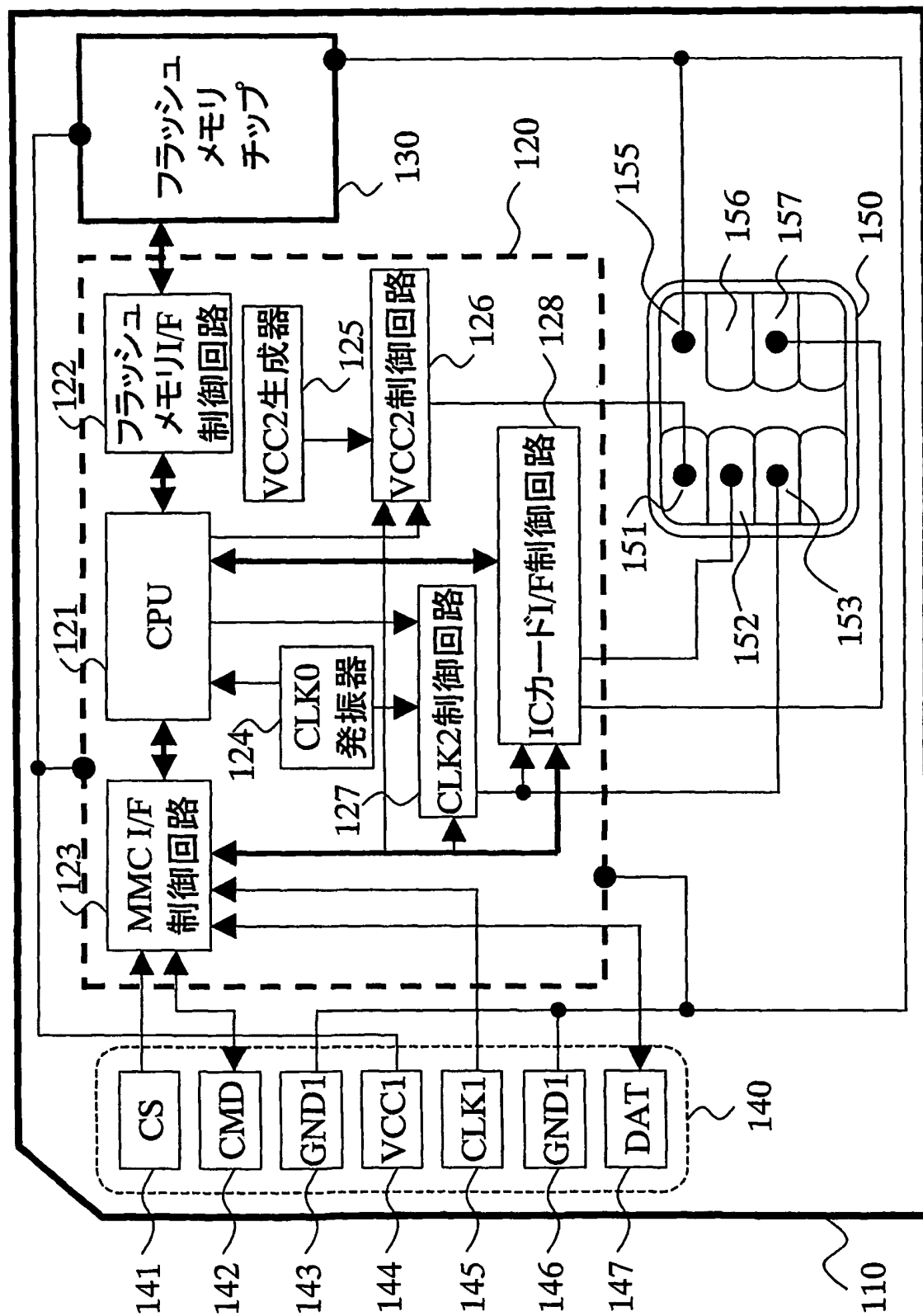


FIG.2

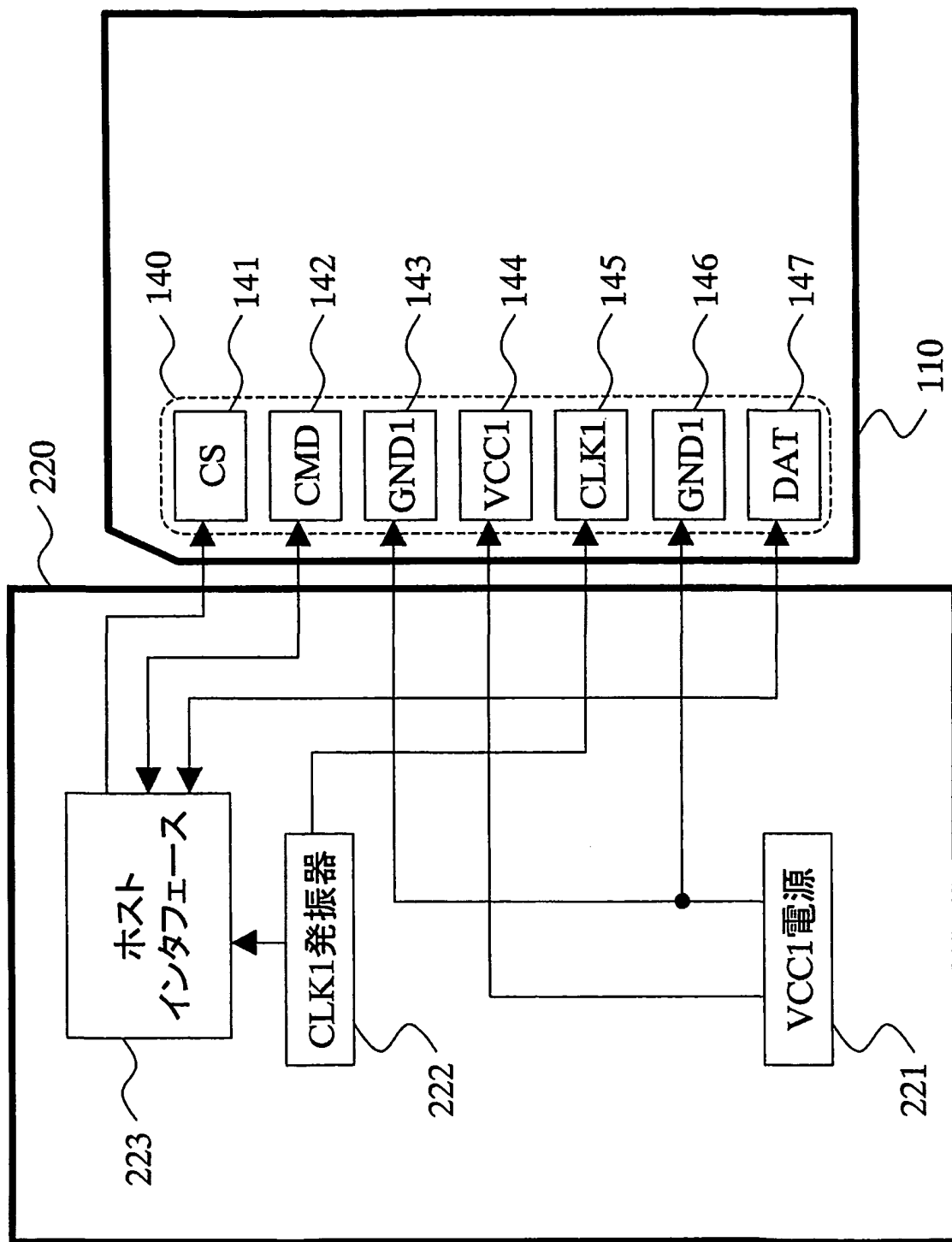


FIG.3

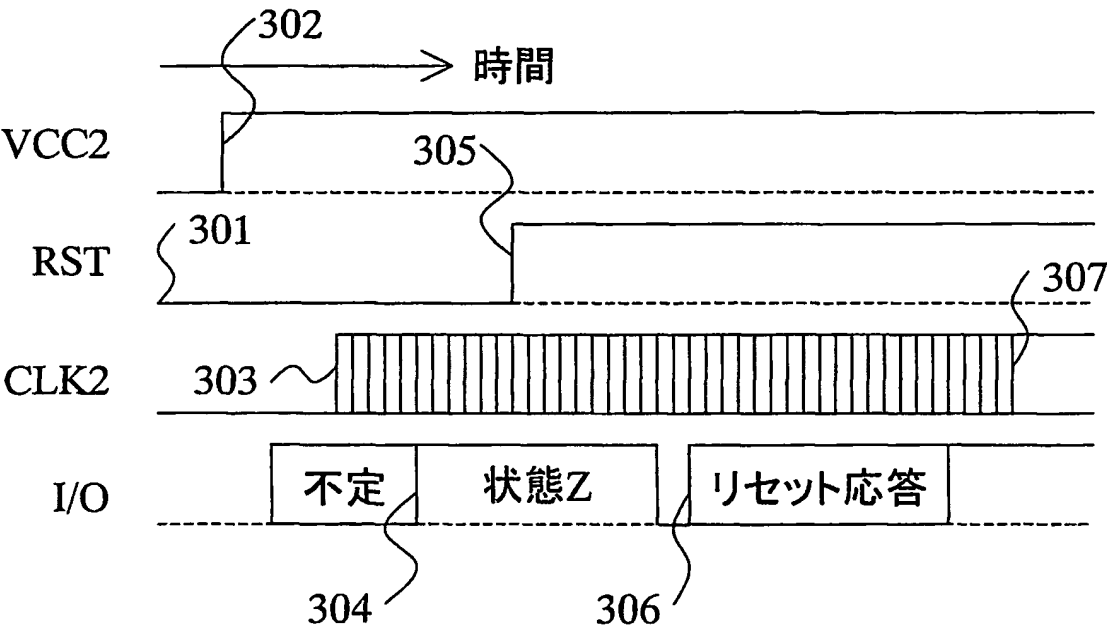
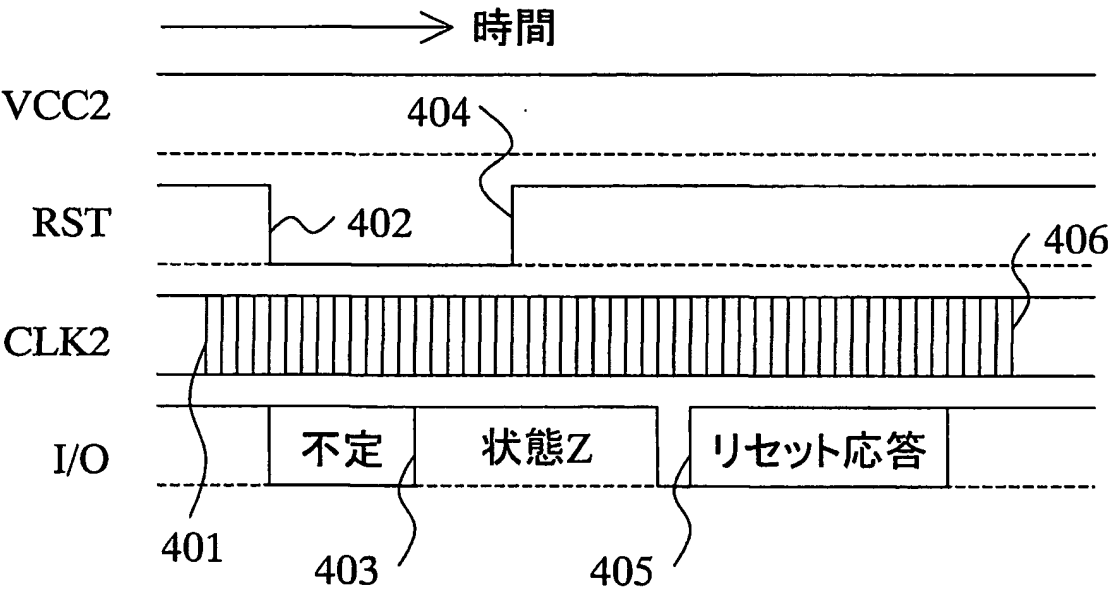
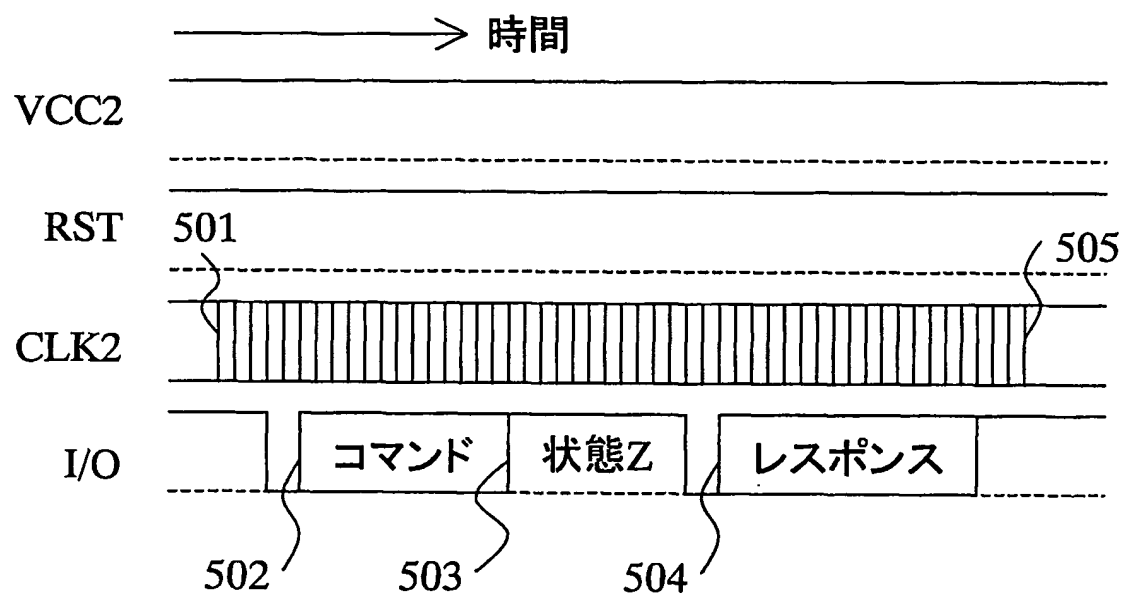


FIG.4



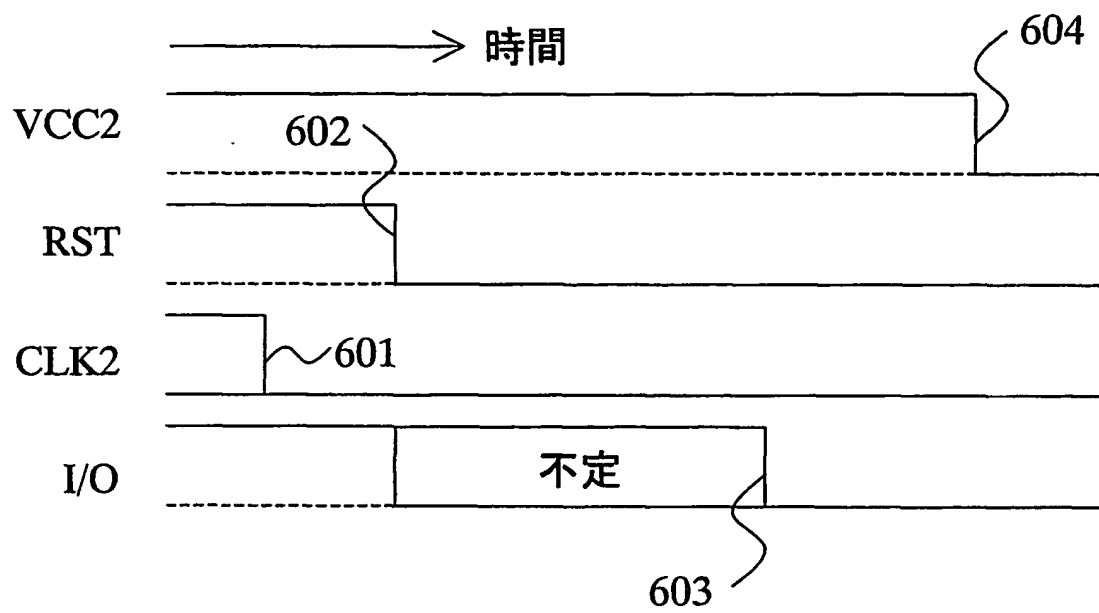
5/27

FIG.5



6/27

FIG.6



7/27

FIG.7

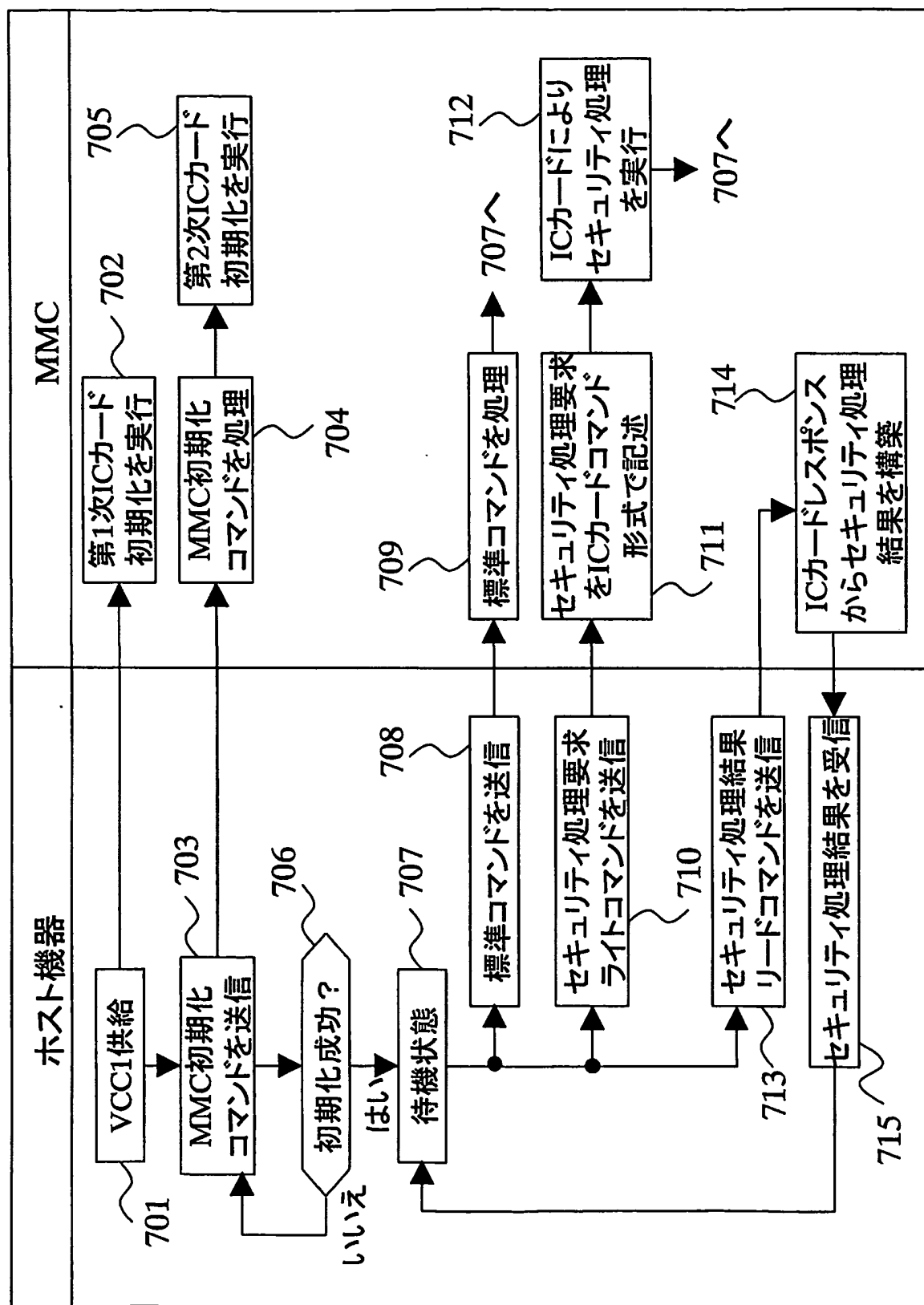
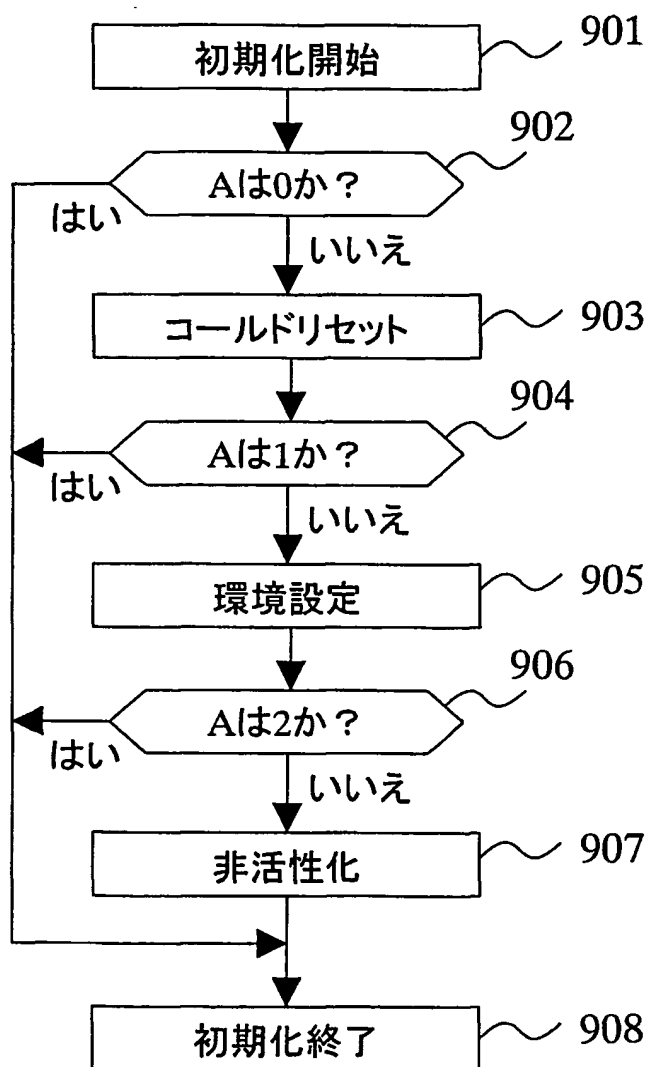


FIG.8

ICカード制御 パラメータ		ICカードに対する処理
A=0		MMCCのパワーオン時に、何もしない
		MMCCのパワーオン時に、リセット
		MMCCのパワーオン時に、リセットと環境設定
A=3		MMCCのパワーオン時に、リセットと環境設定し、非活性化
B=0		MMCCの初期化時に、何もしない
B=1	C=1	MMCCの初期化時に、リセット
	C=2	MMCCの初期化時に、リセットと環境設定
	C=3	MMCCの初期化時に、リセットと環境設定し、非活性化
B=2	C=2	MMCCの初期化時に、環境設定
	C=3	MMCCの初期化時に、環境設定し、非活性化
B=3		MMCCの初期化時に、活性状態ならば、非活性化
D=0		セキュリティ処理後に、非活性化しない
D=1		セキュリティ処理後に、非活性化する

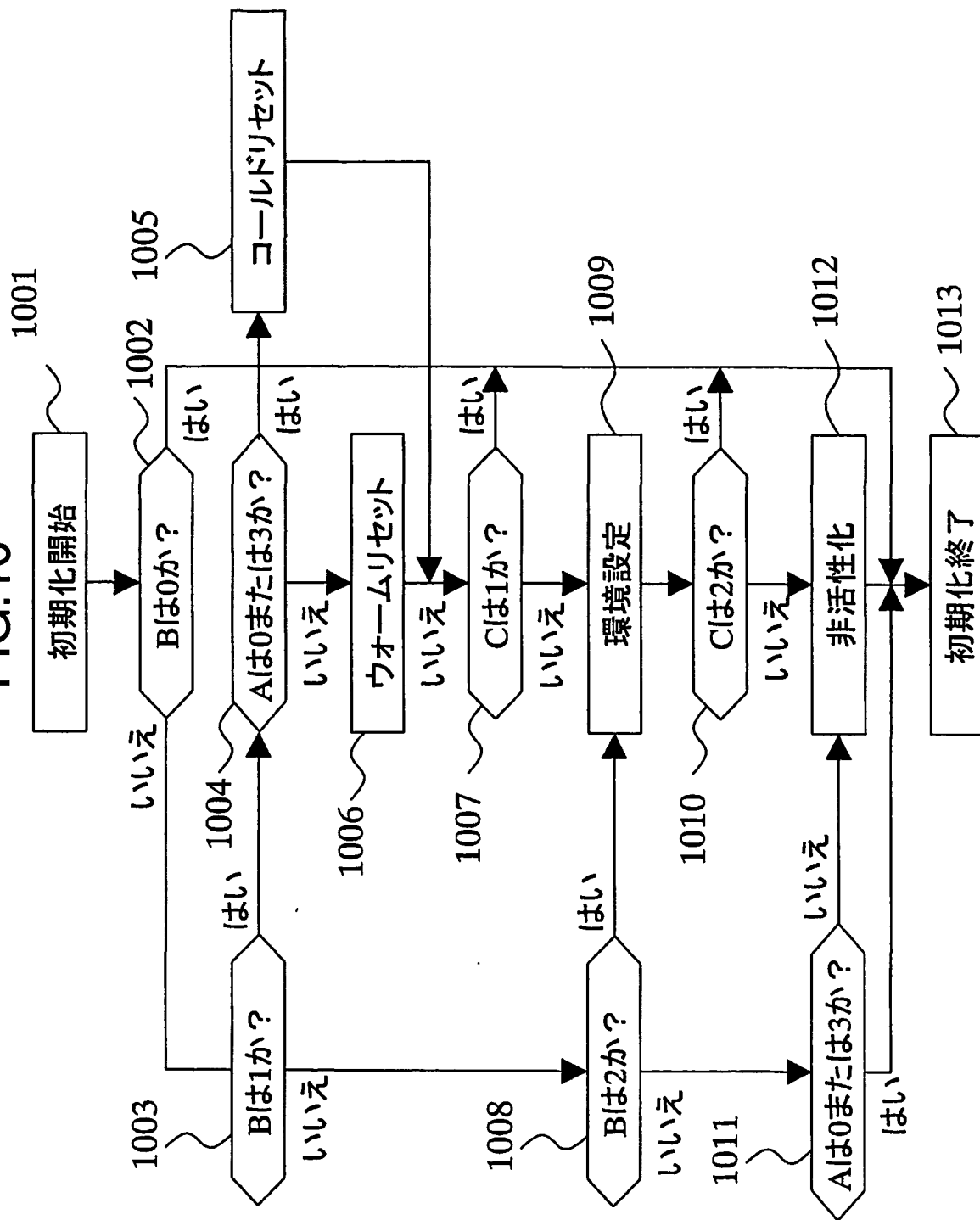
9/27

FIG.9



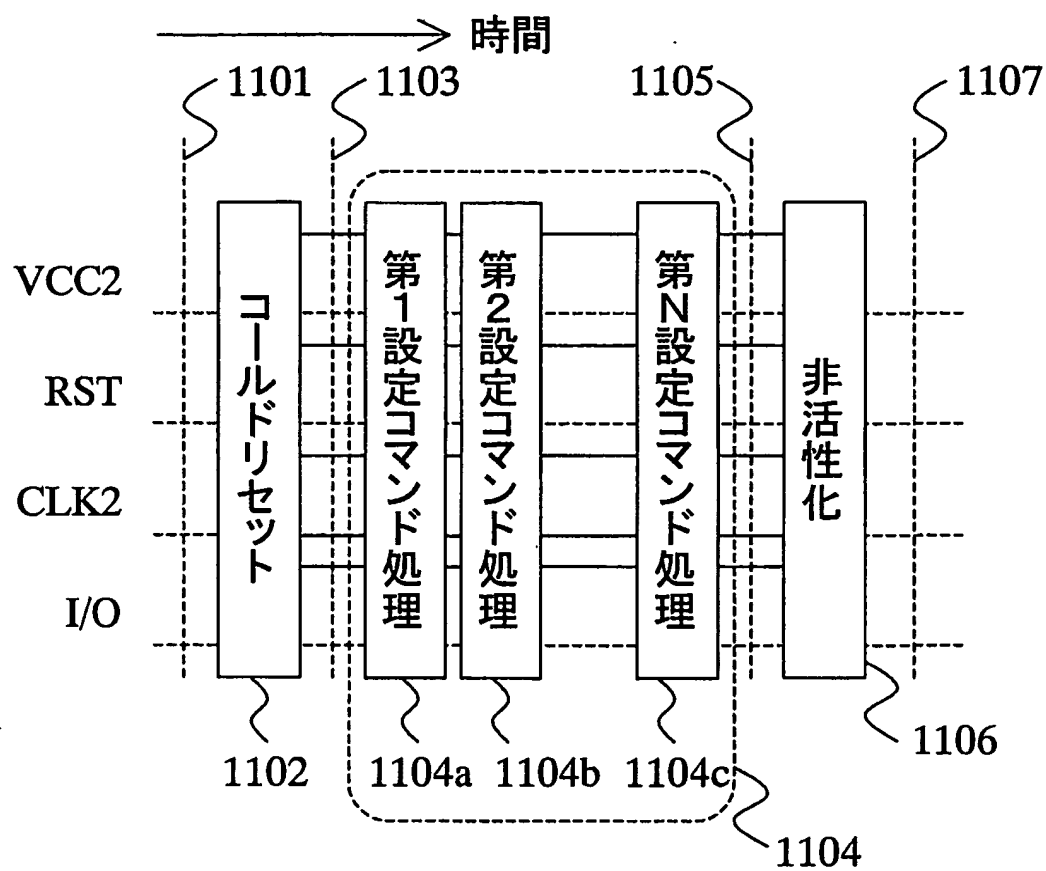
10/27

FIG. 10



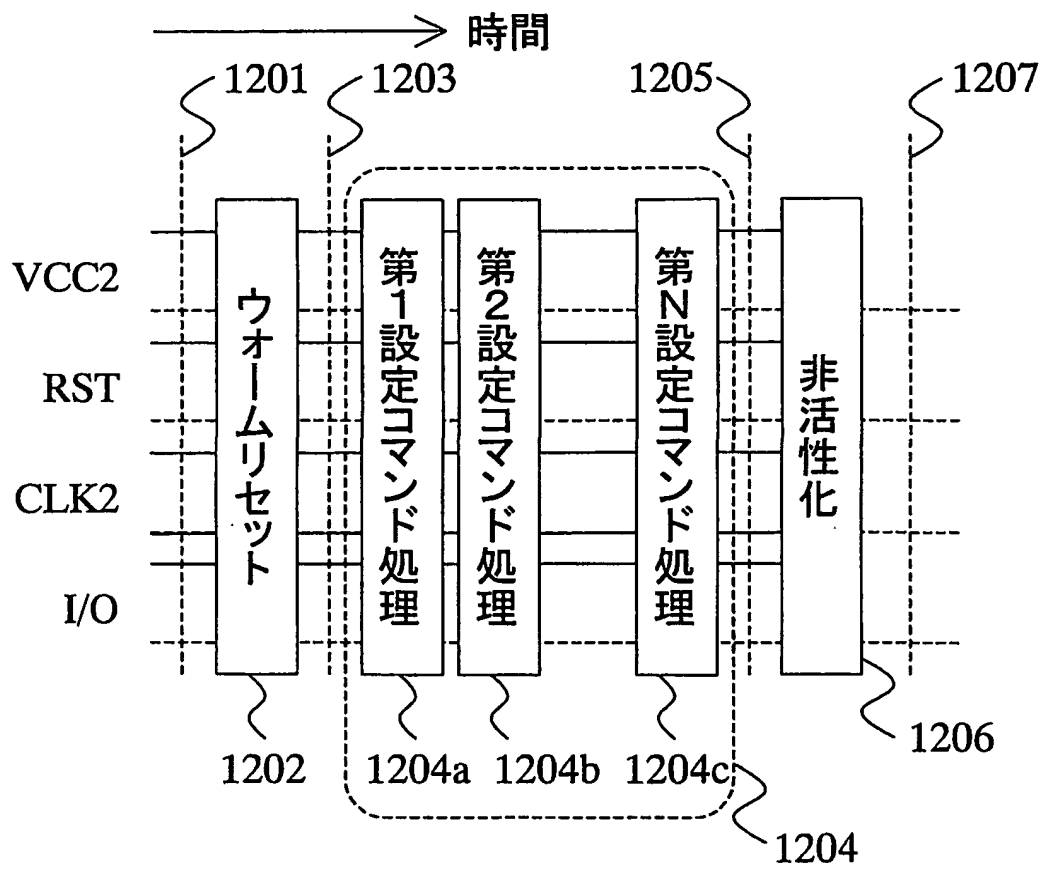
11/27

FIG.11



12/27

FIG.12



13/27

FIG.13

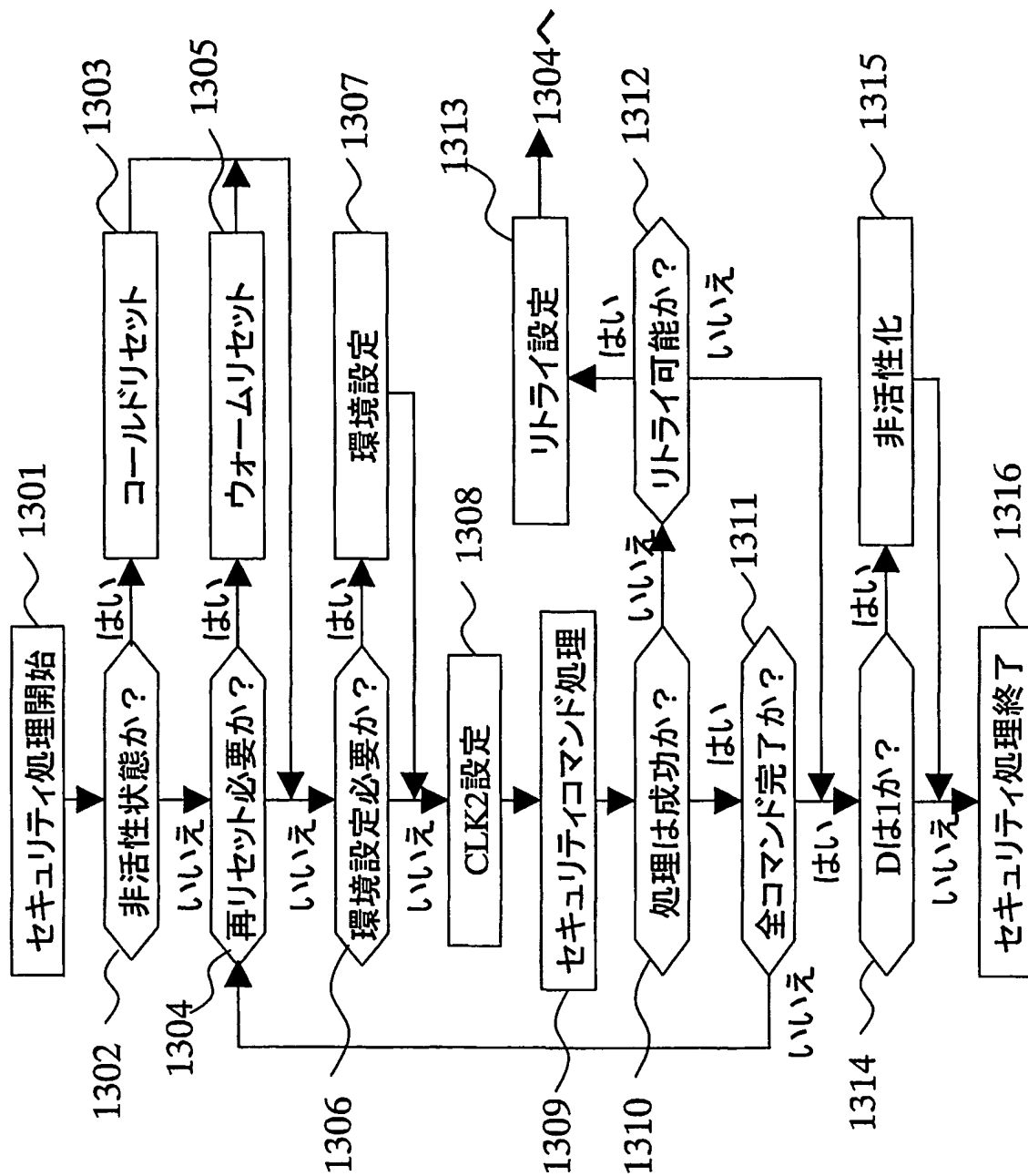


FIG.14

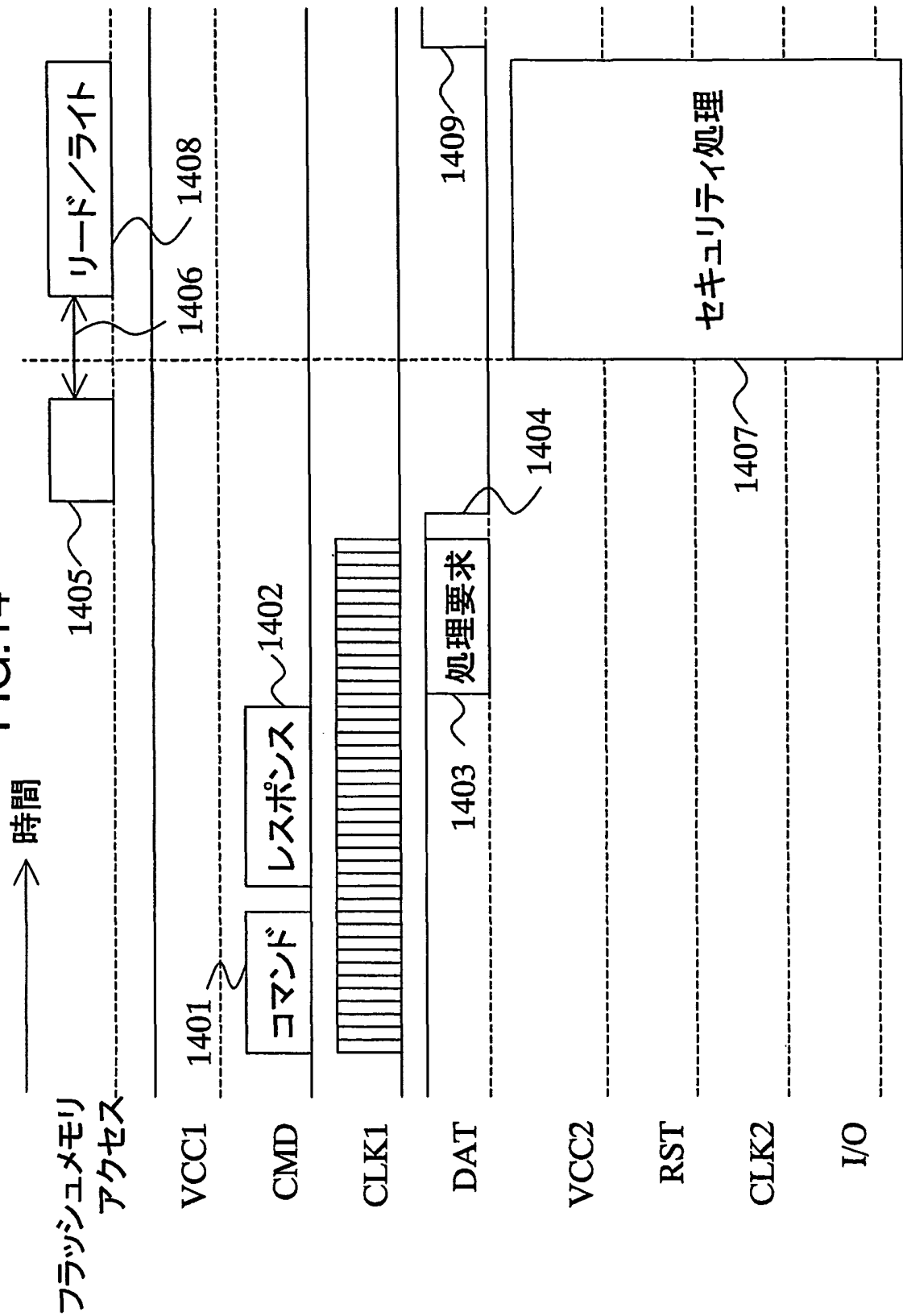


FIG.15

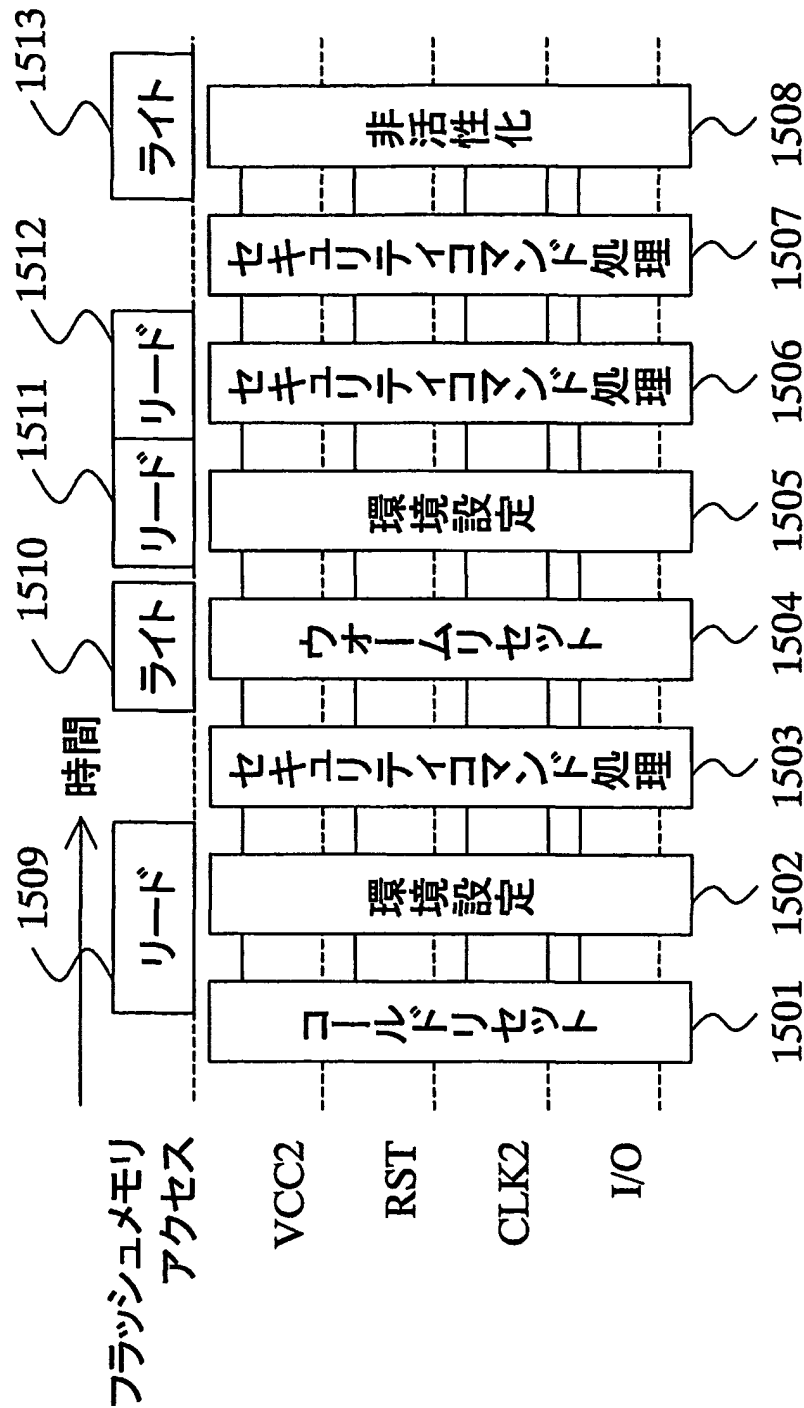
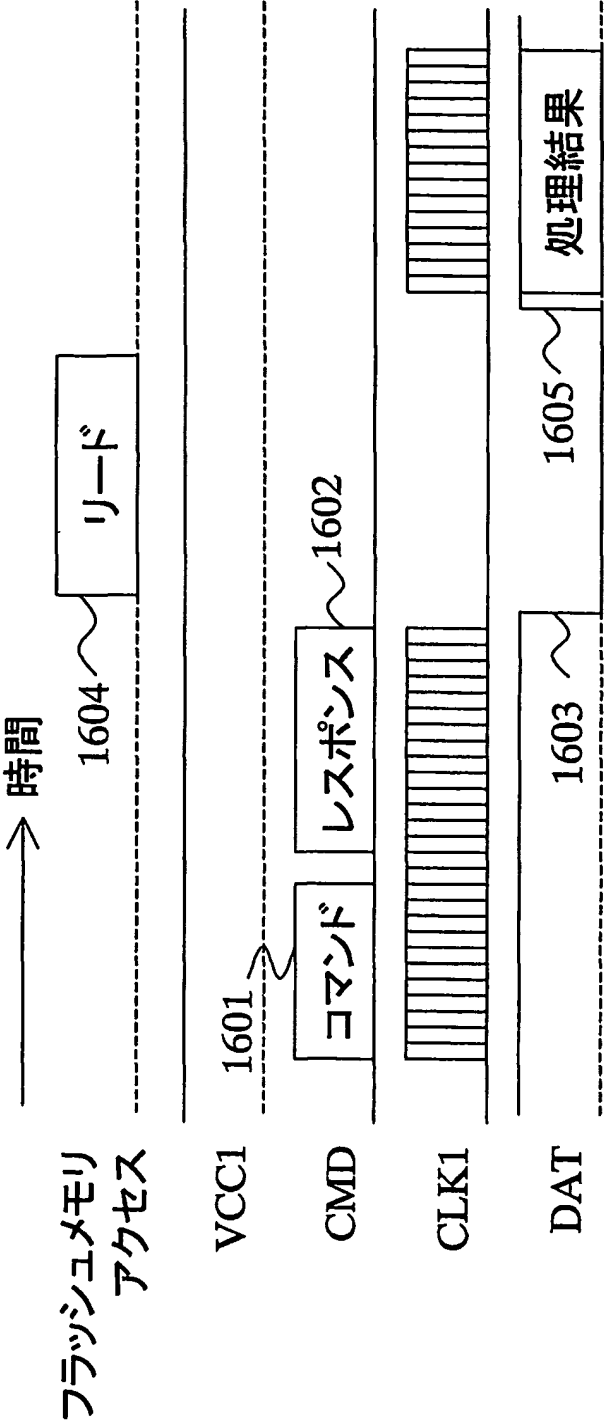
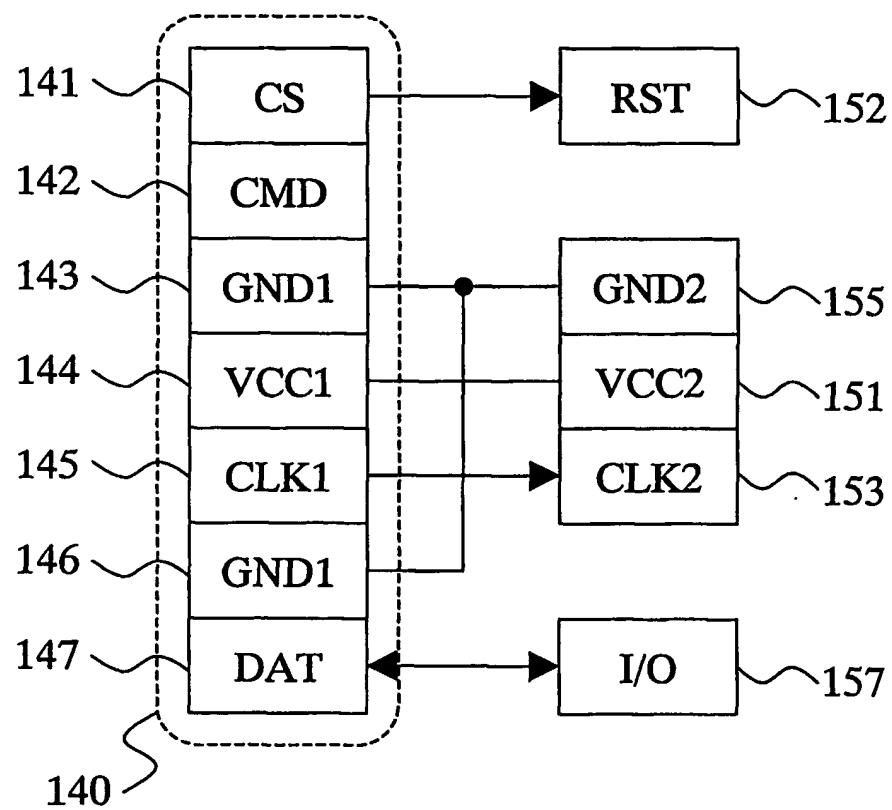


FIG.16



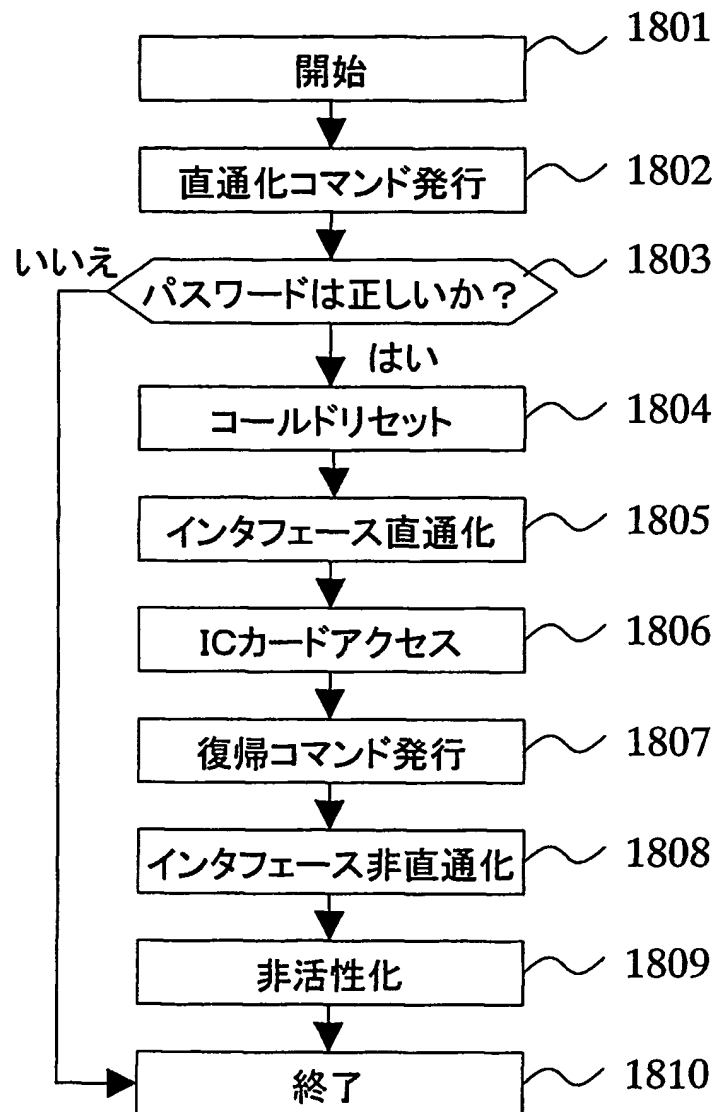
17/27

FIG.17



18/27

FIG.18



19/27

FIG. 19

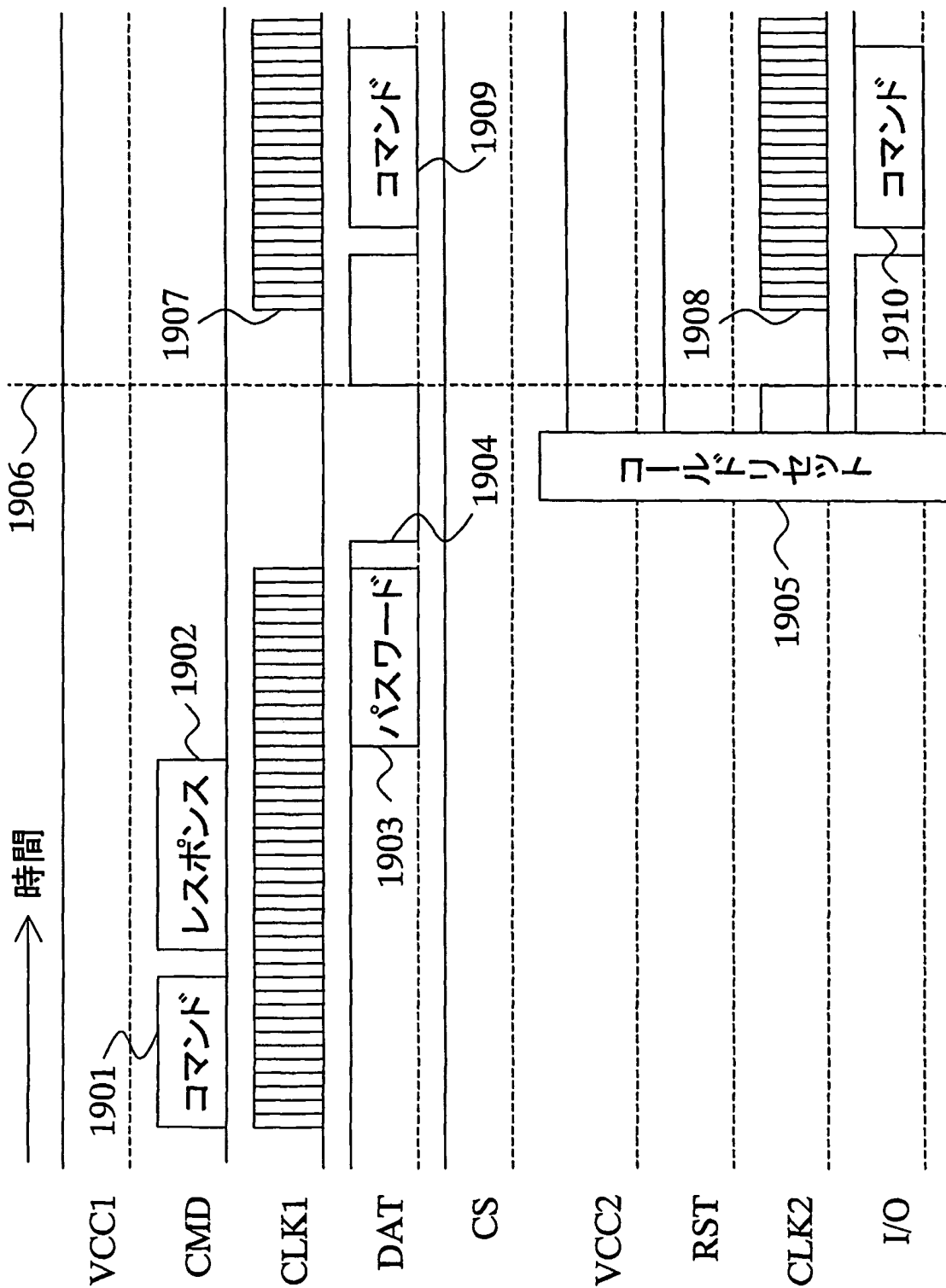


FIG.20

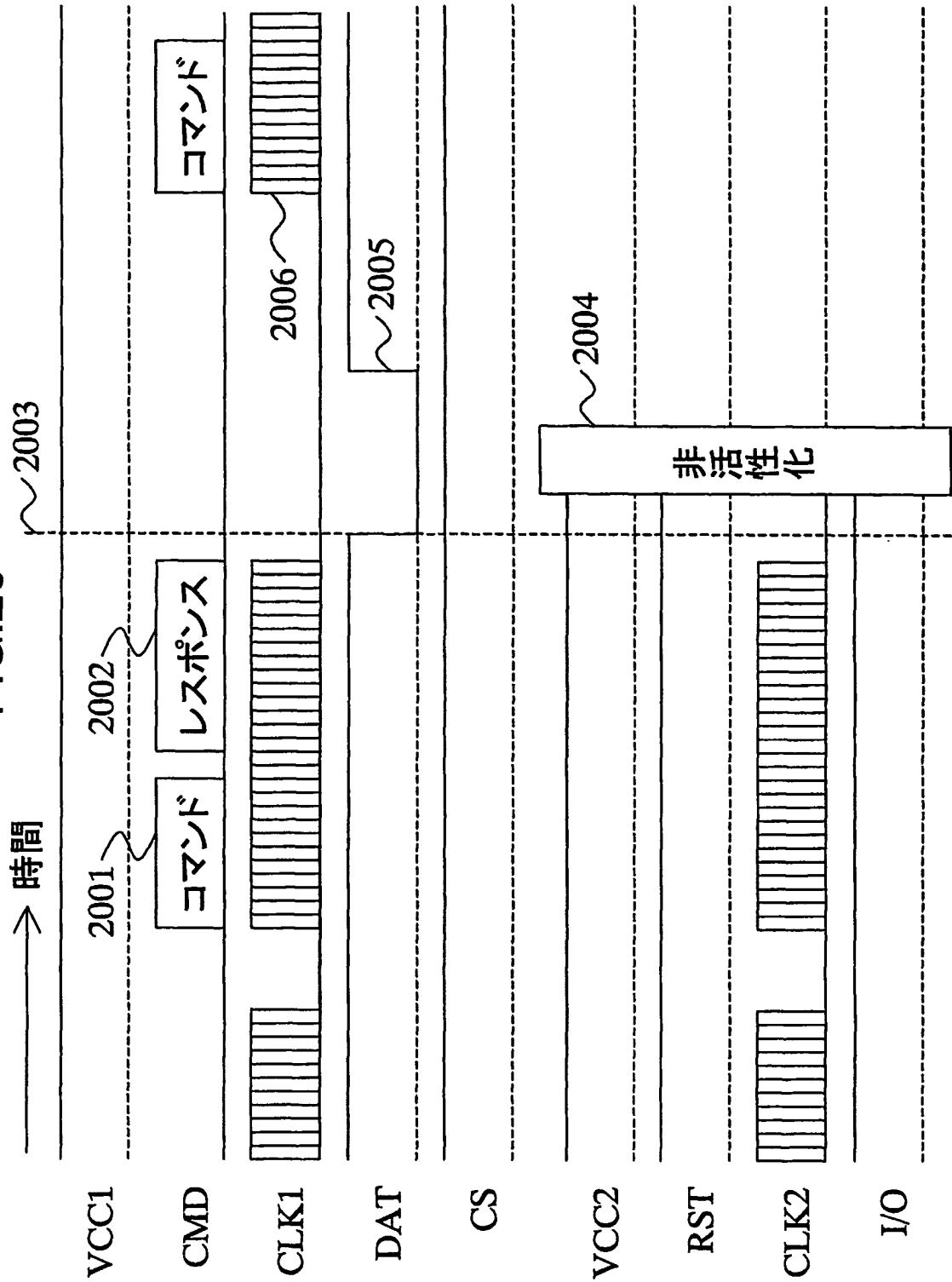
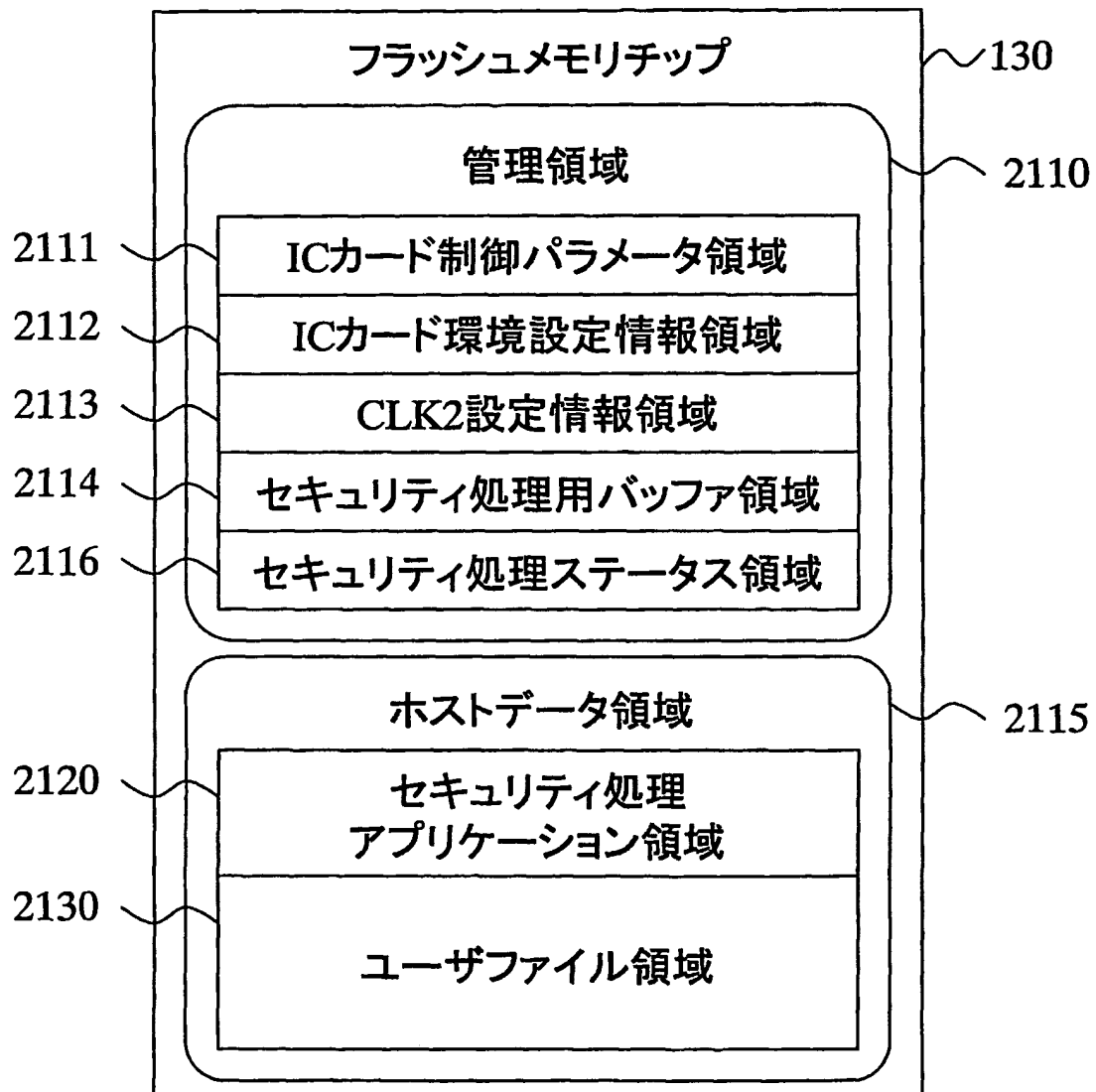


FIG.21



22/27

FIG.22

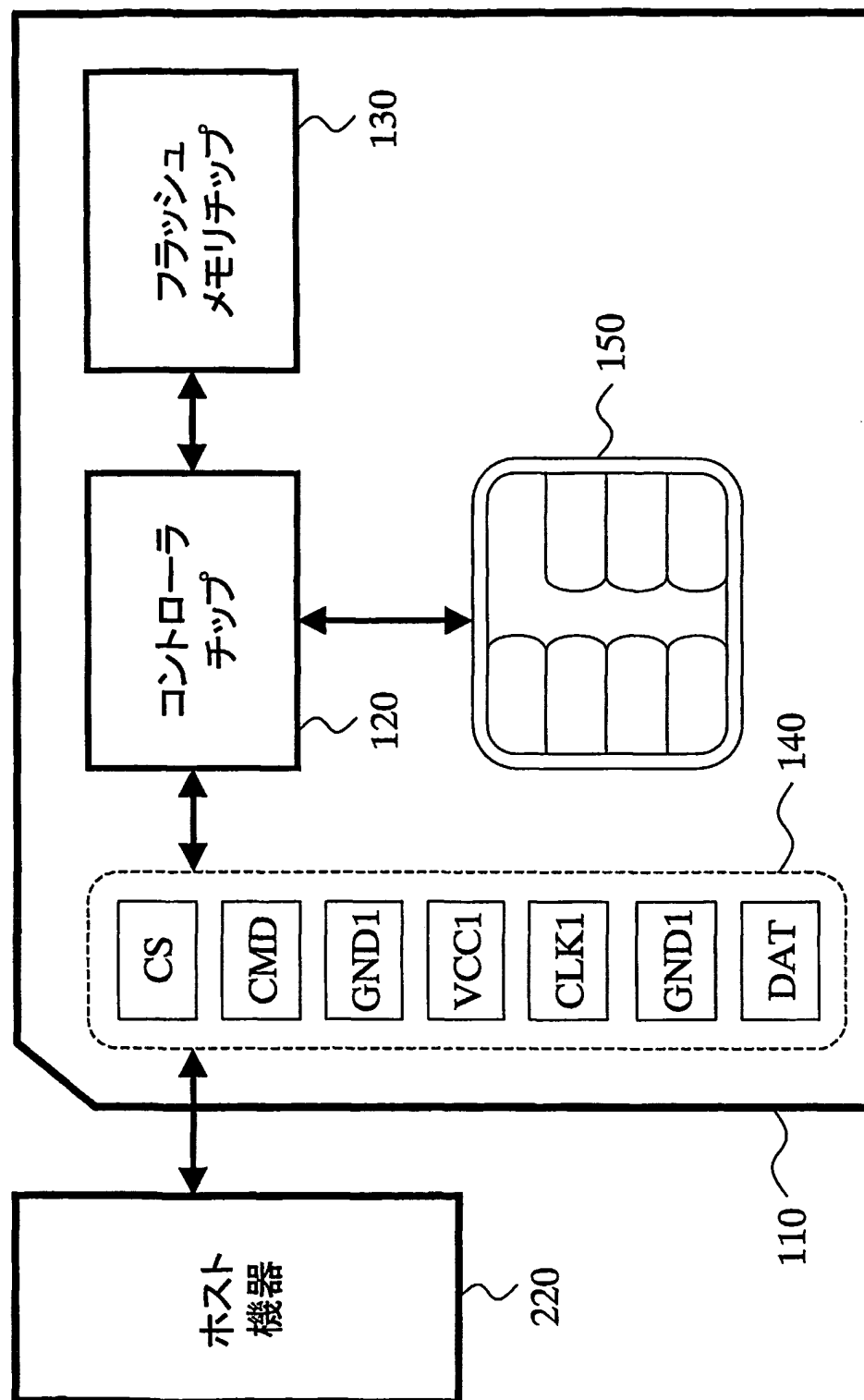


FIG.23

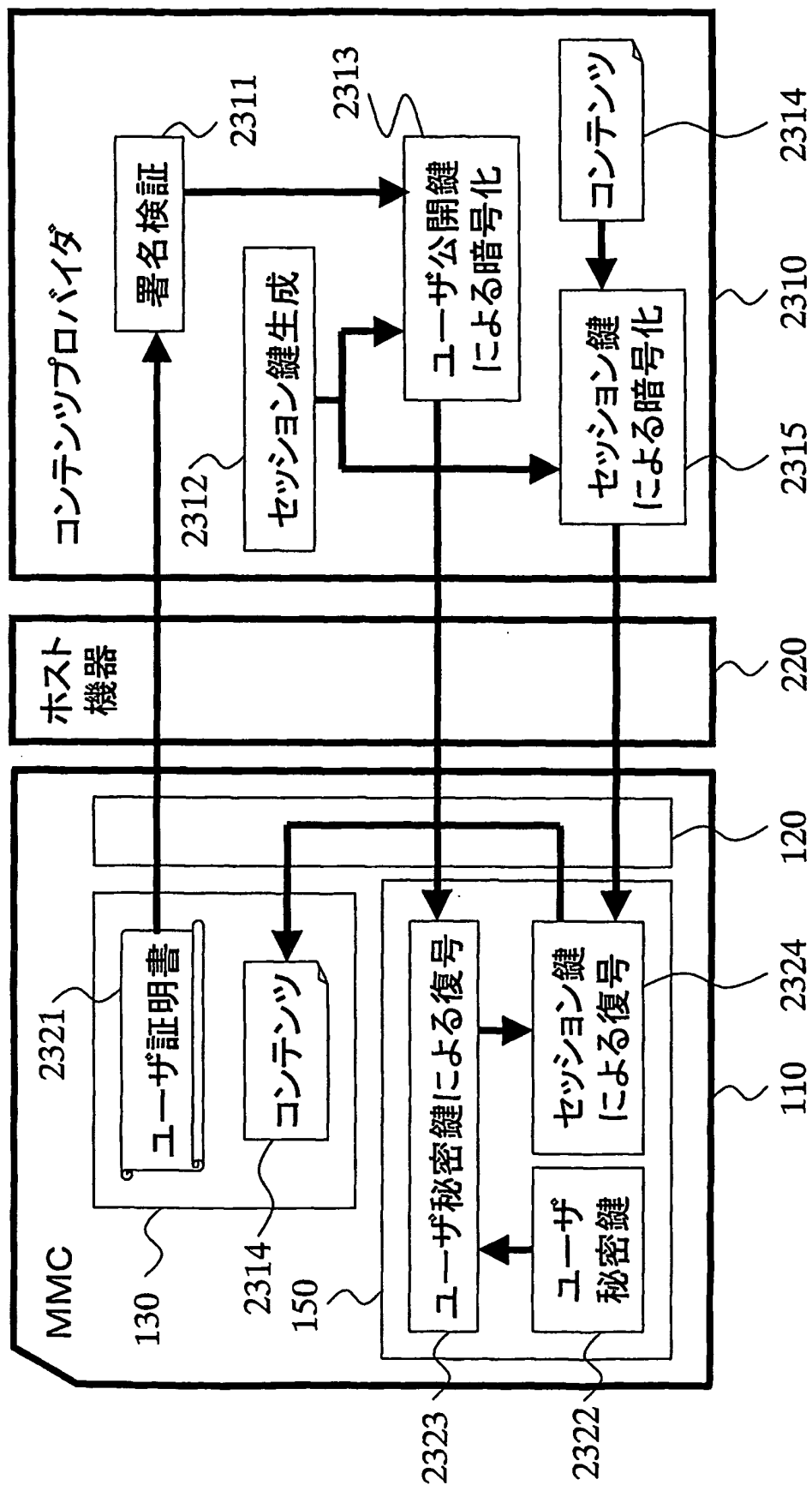
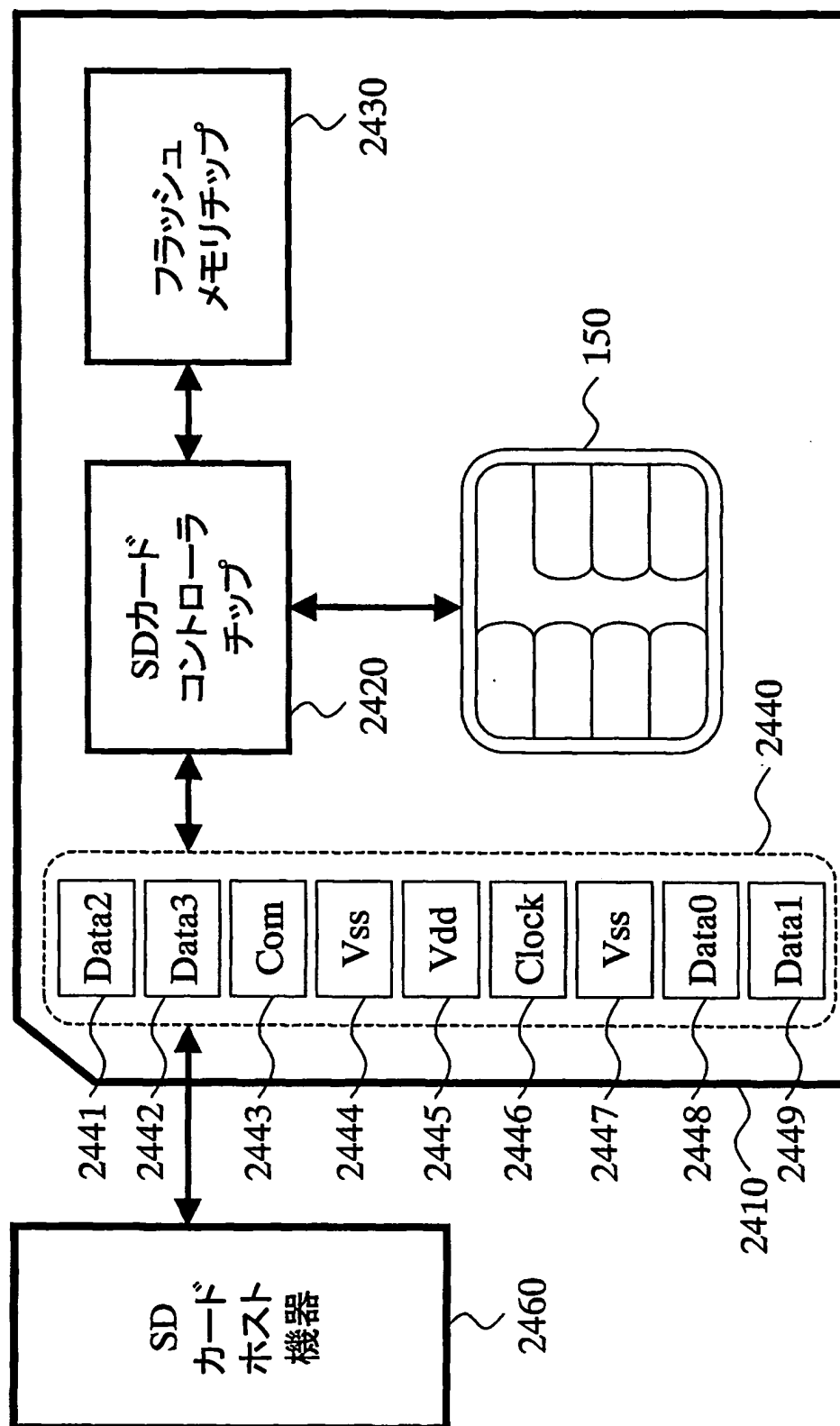


FIG.24



25/27

FIG.25

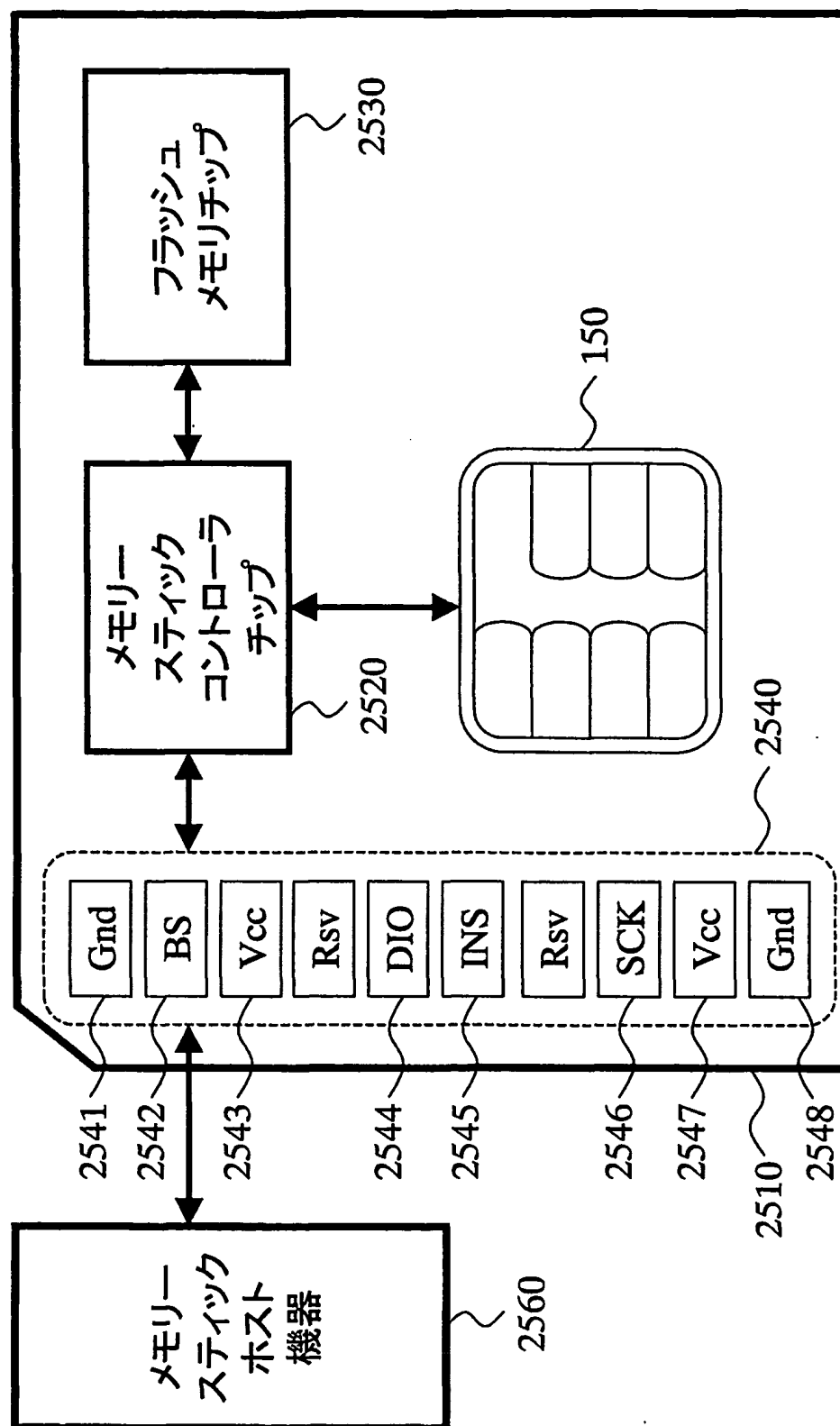


FIG.26

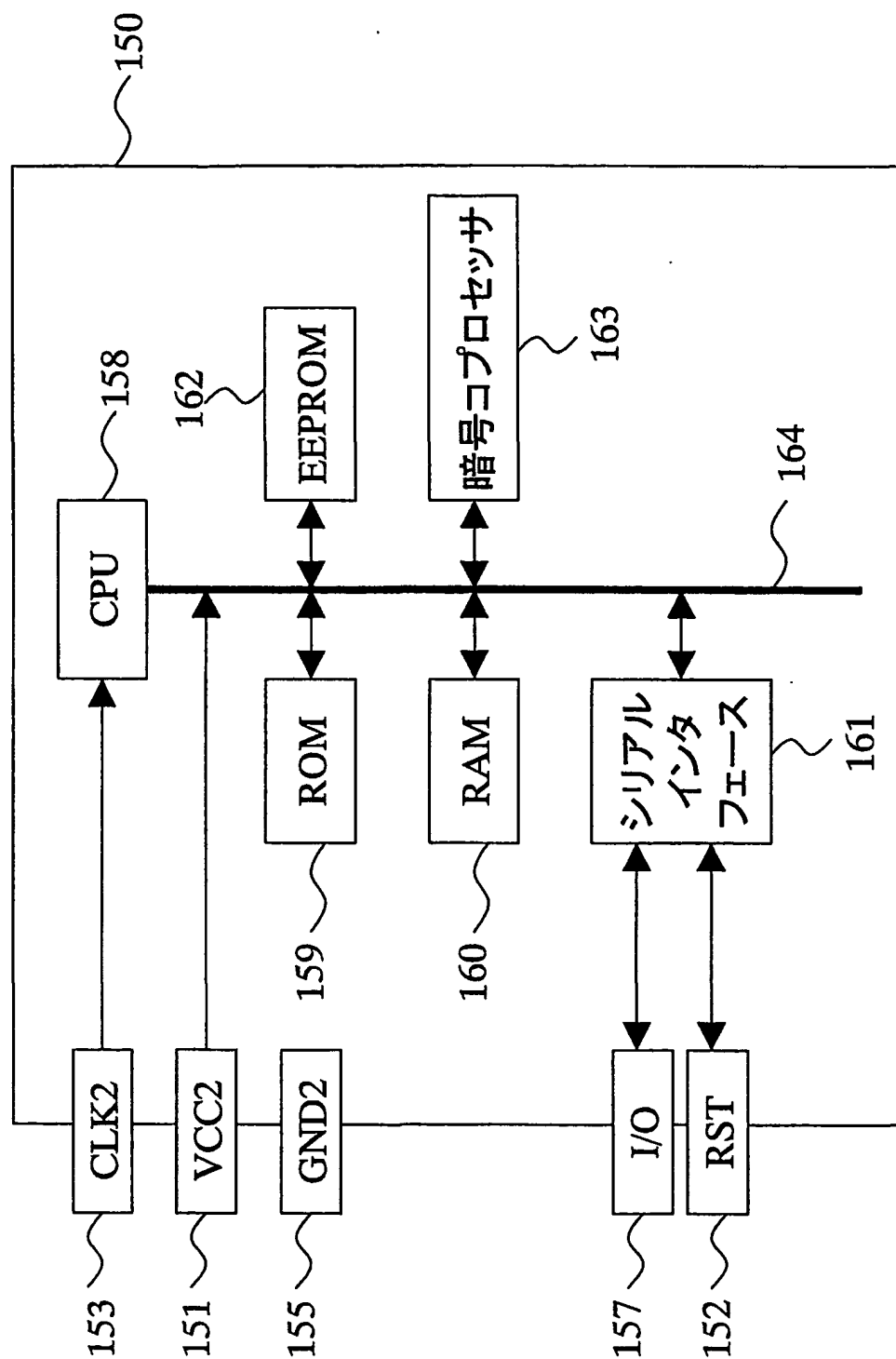
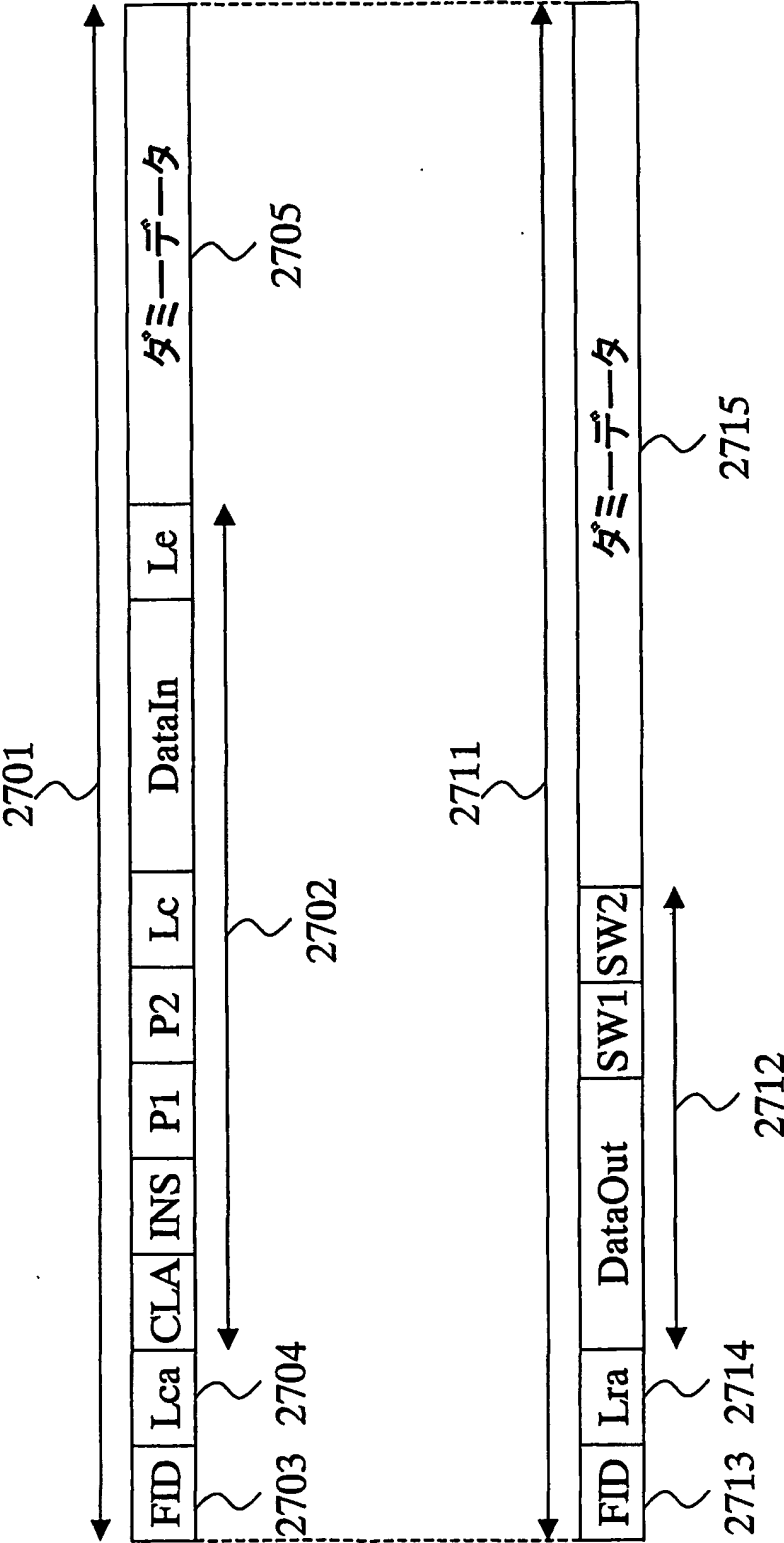


FIG.27



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP02/05236

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ G06K19/073, G06F12/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G06K19/00-19/18, G06F12/14

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2002
Kokai Jitsuyo Shinan Koho	1971-2002	Jitsuyo Shinan Toroku Koho	1996-2002

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	JP 5-314013 A (Gemplus Card International S.A.), 26 November, 1993 (26.11.93), Full text; all drawings & DE 69327181 D & FR 2686170 A & FA 2686170 A1 & EP 552079 A1 & SG 52681 A & US 5875480 A & ES 2142337 T & DE 69327181 T & US 6182205 B1	1-6, 17, 18 7-16, 19
A	JP 8-55200 A (NTT Data Communications Systems Corp.), 27 February, 1996 (27.02.96), Full text; all drawings (Family: none)	1-19

☐ Further documents are listed in the continuation of Box C.
 ☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
04 September, 2002 (04.09.02)Date of mailing of the international search report
24 September, 2002 (24.09.02)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:

because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:

because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:

because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Claims 1 and 2 relate to an IC chip including a device authenticated by an authentication organization.

Claims 3 to 16 relate to a device including a processor capable of executing security processing.

Claims 17 and 18 relate to a device associated with terminal connections.

Claim 19 relates to a device for controlling a processor according to presence/absence of power supply.

These four groups of inventions are not so linked as to form a single general inventive concept.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest ☐ The additional search fees were accompanied by the applicant's protest.

☒ No protest accompanied the payment of additional search fees.

A. 発明の属する分野の分類 (国際特許分類 (IPC))
Int. Cl⁷ G06K19/073, G06F12/14

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))
Int. Cl⁷ G06K19/00-19/18, G06F12/14

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年
日本国公開実用新案公報 1971-2002年
日本国登録実用新案公報 1994-2002年
日本国実用新案登録公報 1996-2002年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X A	JP 5-314013 A(ジェムプリュス カード アンテルナショナル ソシ エテ アノニム) 1993. 11. 26, 全文, 全図 & DE 69327181 D & FR 2686170 A & FA 2686170 A1 & EP 552079 A1 & SG 52681 A & US 5875480 A & ES 2142337 T & DE 69327181 T & US 6182205 B1	1-6, 17, 18 7-16, 19
A	JP 8-55200 A(エヌ・ティ・ティ・データ通信株式会社) 1996. 02. 27, 全文, 全図 (ファミリーなし)	1-19

☐ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日

04. 09. 02

国際調査報告の発送日

24.09.02

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)
郵便番号 100-8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)
奥村 元宏



5 N 8022

電話番号 03-3581-1101 内線 3545

第Ⅰ欄 請求の範囲の一部の調査ができないときの意見 (第1ページの2の続き)

法第8条第3項 (PCT 17条(2)(a)) の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、
2. ☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求の範囲 _____ は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

第Ⅱ欄 発明の単一性が欠如しているときの意見 (第1ページの3の続き)

次に述べるようにこの国際出願に二以上の発明があるところの国際調査機関は認めた。

請求項1～2は、ICチップに認証機関によって予め認証されたものを備えることに係るものであり、
請求項3～16は、セキュリティ処理を実行可能な処理装置を備えることに係るものであり、
請求項17～18は、端子の接続関係に係るものであり、
請求項19は、電源供給の有無に基づく処理装置のコントロールに係るものであり、
これら4つの発明群は単一の一般的発明概念を形成するように連関していない。

1. ☒ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったため、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったため、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。
☒ 追加調査手数料の納付と共に出願人から異議申立てがなかった。